NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CLOSING THE CYBER GAP: INTEGRATING CROSS-GOVERNMENT CYBER CAPABILITIES TO SUPPORT THE DHS CYBER SECURITY MISSION

by

Edward W. Lowery

December 2014

Thesis Advisor: Kathleen Kiernan
Co-Advisor: Lauren Fernandez

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
CLOSING THE CYBER GAP: INTEGRATINGCROSS-GOVERNMENT CYBER CAPABILITIESTO SUPPORT THE DHS CYBER SECURITY MISSION

5. FUNDING NUMBERS

6. AUTHOR(S) Edward W. Lowery

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943–5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

Following the 9/11 terror attacks, the Department of Homeland Security (DHS) was mandated to ensure the security of the nation's cyber-supported critical infrastructure, which is predominantly privately owned and outside of the control of the U.S. government. This thesis examines the development of the government's cyber-security policies and primary operational entities through their lawful authorities and capabilities. The thesis also examines and contrasts the effectiveness of DHS's technology-centric, cyber-security approach, the deterrent effect realized through law enforcement cyber operations, and the suitability and effectiveness of the utilization of military or intelligence agencies, specifically the FBI, National Security Agency or Department of Defense, to fulfill the nation's domestic cyber-security mission.

Evidence suggests that DHS has consistently chosen to devote disproportionate budgetary resources to develop defensive technologies of questionable effectiveness, initiate redundant information-sharing programs, and develop cyber incidence response teams while not fully utilizing the U.S. Secret Service's legal authorities and capabilities in furtherance of the department's mission.

Recommendations are offered to develop a whole-of-government cyber-security policy for an effective, integrated, cyber-security operation through the utilization of agency-specific authorities and capabilities, while protecting our nation's critical infrastructure and our citizens' civil liberties.

14. SUBJECT TERMS Cybersecurity, U.S. Secret Service, Department of Homeland Security, DHS

15. NUMBER OF PAGES
139

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01–280–5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

CLOSING THE CYBER GAP: INTEGRATING CROSS-GOVERNMENT CYBER CAPABILITIES TO SUPPORT THE DHS CYBER SECURITY MISSION

Edward W. Lowery
Special Agent in Charge, United States Secret Service
B.S., University of North Carolina at Charlotte, 1991

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
December 2014

Author: Edward W. Lowery

Approved by: Kathleen Kiernan, Ed.D.
Thesis Advisor

Lauren Fernandez, D.Sc.
Co-Advisor

Mohammed Hafez, Ph.D.
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Following the 9/11 terror attacks, the Department of Homeland Security (DHS) was mandated to ensure the security of the nation's cyber-supported critical infrastructure, which is predominantly privately owned and outside of the control of the U.S. government. This thesis examines the development of the government's cyber-security policies and primary operational entities through their lawful authorities and capabilities. The thesis also examines and contrasts the effectiveness of DHS's technology-centric, cyber-security approach, the deterrent effect realized through law enforcement cyber operations, and the suitability and effectiveness of the utilization of military or intelligence agencies, specifically the FBI, National Security Agency or Department of Defense, to fulfill the nation's domestic cyber-security mission.

Evidence suggests that DHS has consistently chosen to devote disproportionate budgetary resources to develop defensive technologies of questionable effectiveness, initiate redundant information-sharing programs, and develop cyber incidence response teams while not fully utilizing the U.S. Secret Service's legal authorities and capabilities in furtherance of the department's mission.

Recommendations are offered to develop a whole-of-government cyber-security policy for an effective, integrated, cyber-security operation through the utilization of agency-specific authorities and capabilities, while protecting our nation's critical infrastructure and our citizens' civil liberties.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AD	Assistant Director
AG	Attorney General
BUR	*Bottoms-Up Review*
CERT-CC	Carnegie Mellon-Computer Emergency Response Team
CFAA	Computer Fraud and Abuse Act of 1986
CI	Counter Intelligence
CIA	Central Intelligence Agency
CIKR	Critical Infrastructure and Key Resources
CNA	Cyber Network Attack
CNCI	Comprehensive National CyberSecurity Initiative
COMINT	Communications Intelligence
CSIS	Center for Strategic and International Studies
CSPI	Critical Systems Protection Initiative
CTF	Cyber Task Forces
CYBERCOM	Cyber Command
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DHS-OIG	Department of Homeland Security Office of the Inspector General
DOD	Department of Defense
DOJ	Department of Justice
DSAIC	Deputy Special Agent in Charge
ECTF	Electronic Crimes Task Force
EO	Executive Order
EOP	Executive Office of the President
ESF	Enduring Security Framework
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FISA	Foreign Intelligence Surveillance Act
FO	Field Offices
FS-ISAC	Financial Services Information Sharing and Analysis Center
FTE	Full Time Equivalent
GAO	Government Accountability Office
HSA	Homeland Security Act of 2002
HSC	Homeland Security Council
HSPD	Homeland Security Presidential Directive

IC	Intelligence Community
ICE	Immigration and Customs Enforcement
ICE-HSI	Immigration and Customs Enforcement Homeland Security Investigation
IDS	Intrusion Detection System
ILP	Intelligence Led Policing
IP	Infrastructure Protection
IPS	Intrusion Prevention System
ISAC	Information Sharing and Analysis Center
JTTF	Joint Terror Task Force
NCCIC	National Cyber and Communication Integration Center
NCFI	National Computer Forensics Institute
NCIJTF	National Cyber Investigative Joint Task Force
NCSD	National Cyber Security Division
NIPP	National Infrastructure Protection Plan
NPPD	National Protection and Programs Directorate
NS	National Security
NSA	National Security Agency
NSC	National Security Council
NSCID	National Security Council Intelligence Directive
NSD	National Security Division
NSPD	National Security Presidential Directive
NTAC	National Threat Assessment Center
ODNI	Office of the Director of National Intelligence
PCCIP	Presidents Commission on Critical Infrastructure Protection
PPD	Presidential Decision Directive
QHSR	*Quadrennial Homeland Security Review*
R&D	Research and Development
SAIC	Special Agent in Charge
SECDEF	Secretary of Defense
SIGINT	Signals Intelligence
SSD	Secret Service Division
TELINT	Telemetry Intelligence
TS	Top Secret
TTP	Tactic, Techniques and Procedures
USC	United States Code

U.S.-CERT	United States Computer Emergency Response Team
USCG	United States Coast Guard
USSID	United States Signals Intelligence Directive
USSS	United States Secret Service
WMD	Weapons of Mass Destruction

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Since the initial development of the Internet as an information-sharing platform, the cyber world has grown exponentially and become intertwined with almost every facet of our daily activities, commerce, and governmental operations. But, increasingly, the opportunities offered by the cyber world have resulted in rapidly increasing threats to our citizens, businesses and government operations.

Cyber security and cyber law enforcement operations were recognized as rapidly growing fields when the nation suffered the terrorist attacks of September 11, 2001. Following the attacks, the U.S. government worked to reassure the American public, mitigate previously unidentified threats, and provide for citizens' safety and security. During this time, many organizational changes were made to facilitate increased security and operational efficiency. Among the most significant was the creation of the Department of Homeland Security (DHS) with the passage of Public Law 107–296 (Homeland Security Act of 2002) on November 25, 2002.

On September 11, 2001, the U.S. Secret Service (USSS) was operationally aligned within the U.S. Treasury Department with the authorities conferred since its formation in 1865 to suppress the counterfeiting of U.S. currency. The USSS has continued to develop its investigative expertise as the primary investigative agency defending the nation's financial infrastructure through financial crimes investigations. Over the course of its history, the Secret Service's investigative authorities evolved, and the agency adapted its capabilities to account for changing technologies that supported the nation's critical financial infrastructure. As the financial sector became increasingly reliant on cyber technologies, and the threats emanating from cyberspace became more pervasive, the USSS also consistently increased its investment in cyber-investigative capabilities. The USA Patriot Act, which passed on October 26, 2001, called for an expansion of the USSS Electronic Crime Task Force (ECTF) model, which had been proven to be a successful method of investigating the terrorist use of cyber technologies

and the prevention of attacks against the nation's financial infrastructure through aggressive enforcement and information sharing.[1]

In 2003, the USSS, although mandated to remain a distinct agency operating within its own authorities, was transferred to the Department of Homeland Security (DHS), whose mission was to ensure the security of the nation from terrorist attack.[2] Since that time, DHS's mission has expanded to include the security and resilience of the nation's 16 Critical Infrastructure And Key Resources (CIKR), which includes the financial infrastructure and cyberspace.[3] DHS's National Protection and Programs Directorate (NPPD) was formed to coordinate the department's cyber-security mission but, as reflected in multiple governmental reports, NPPD has underutilized DHS component cyber-security capabilities, namely the USSS cyber investigation expertise, to further the department's cyber-security mission.[4]

This thesis documents the U.S. government's post-9/11 initial focus on the threat posed by international terrorism to its shifting focus on the nation's resiliency, and finally, to cyber-based threats that could impact the nation's identified critical infrastructure. It examines the Department of Homeland Security as it followed the identical development process, as well as the operations and development of the primary cyber law enforcement, military and intelligence agencies supporting this cyber security effort.

Research questions were developed to guide this research and, ultimately, provide recommendations to assist the U.S. government in developing a comprehensive national cyber security methodology and policies that utilize agency-specific lawful authorities

---

[1] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[2] An Act to Establish the Department of Homeland Security, and for Other Purposes (Homeland Security Act) Act of 2002, Pub. L. No. 107-296 Stat. 2135 (2002).

[3] U.S. Department of Homeland Security (DHS), *National Infrastructure Protection Plan*, (Washington, DC: DHS, 2009) https://www.dhs.gov/national-infrastructure-protection-plan.

[4] Frank Deffer, *Planning, Management, and Systems Issues Hinder DHS' Efforts To Protect Cyberspace and the Nation's Cyber Infrastructure* (OIG -11-89) (Washington, DC: OIG and DHS, June 2011), https://www.hsdl.org/?view&did=683172.

and capabilities to strengthen our cyber security efforts while protecting our citizens' civil liberties and privacy.

- **Primary research question:** What strategies can the U.S. government develop that support the efforts of DHS, in concert with other governmental cyber security entities, to ensure the nation's cyber-supported critical infrastructure is provided with the most comprehensive security, while ensuring our citizens' privacy and security are preserved?
- **Secondary research question:** How could the application of established law enforcement investigative authorities and capabilities augment the technology-centric, defensive cyber methods currently utilized by the Department of Homeland Security to secure the nation's critical infrastructure against criminal cyber intrusions?

Through a review of DHS budgetary documents, evidence suggests that DHS has consistently chosen to devote disproportionate budgetary resources to develop defensive technologies of questionable effectiveness, initiate redundant information-sharing programs, and to develop cyber incidence response teams, while not considering the utilization of component agency's legal authorities and capabilities, namely the U.S. Secret Service. The underutilization of the department's own cyber law enforcement component's capabilities has arguably affected the overall effectiveness and efficiency of the department's efforts. The analysis indicates that the USSS has the expertise and legal mandate to integrate the traditional model of criminal investigation and deterrence to the realm of cyber security and better support the DHS mission.

Cyber-law enforcement effectiveness was also contrasted against the suitability and effectiveness of utilizing intelligence or military agencies to fulfill the nation's domestic cyber-security mission. As Steven Tomisek described in his 2002 report *Homeland Security: The New Role for Defense*, since 9/11, government agencies, predominantly represented by the National Security Agency (NSA) and Department of Defense (DOD), have aggressively promoted the premise that any cyber threat targeting our nation's critical infrastructure, including the financial infrastructure, should be designated as a "national security" threat, regardless of the motivations or identity of the

attacker.[5] The NSA and DOD have argued that they alone possess the requisite capabilities to successfully counter this critical threat to our national security through domestic and international cyber operations. Evidence presented in this thesis indicates that DHS's apparent acceptance of the premise that NSA/DOD should provide domestic technical assistance, cyber security support, and mitigation may be in violation of existing laws prohibiting domestic operations by the intelligence community and military.

Additionally, as argued by Tyler Moore, Allan Friedman and Ariel D. Procaccia in "Would a 'Cyber Warrior' Protect Us?: Exploring Trade-offs between Attack and Defense of Information Systems," relying on the intelligence community (IC) and military cyber attack units to provide effective defensive information and technology may be a faulty assumption because providing that information would be counter to the IC and military's primary missions and negatively affect their overall effectiveness.[6] The analysis indicated that the government's proposed designation of all cyber attacks targeting the nation's critical infrastructure as a "national security" event was initiated and fully supported by the IC and military. This designation, regardless of the identity or motivations of the perpetrator, was described within this thesis as a thinly veiled attempt to provide justification for the NSA/DOD to operate domestically despite the fact that the FBI is the only agency legally authorized to conduct domestic intelligence operations to counter national security threats. Finally, this proposal by the IC was presented as an effort that could threaten our citizens' privacy due to the lack of intelligence community operational oversight and the borderless nature of the cyber world.

This thesis, and supporting research, offers comparative information to support the formulation of government cyber-security policy that develops the most effective, integrated cyber-security methods while protecting civil liberties and our citizens'

---

[5] Steven J. Tomisek, *Homeland Security: The New Role for Defense* (Washington, DC: Institute for National Strategic Studies, National Defense University, 2002).

[6] Tyler Moore, Allan Friedman, and Ariel D. Procaccia, "Would a 'Cyber Warrior' Protect Us?: Exploring Trade-Offs between Attack and Defense of Information Systems," in *Proceedings of the 2010 Workshop on New Security Paradigms* (New York: 2010 ACM, 2010), 85–94, doi:978-1-4503-0415-3.

privacy. This thesis then offers policy recommendations to assist in this whole of government cyber security effort. These recommendations include:

- **DOD/NSA must remain focused on nation-state cyber threats and foreign activities.** To ensure that the NSA, the nation's premier SIGINT collection agency, remains focused on the exploitation of foreign SIGINT and foreign espionage activities in support of our national security interests, as well as to protect our citizens' civil liberties, the agency must not be permitted to utilize its capabilities on domestic targets or systems. Additionally, the DOD cyber attack forces must not operate on or within domestic cyber systems, unless owned by the DOD, and must concentrate their activities to exploiting foreign vulnerabilities.
- **FBI must remain the only IC agency permitted to operate domestically with proper judicial oversight.** The bureau's domestic cyber intelligence activity must be limited to the investigation of espionage threats which are committed by nation-state supported actors that 1.) Seek to gain knowledge from information systems which contain information of national security value or; 2.) Attack critical infrastructure systems to degrade or disrupt such systems to cause a national crisis. The FBI Cyber Criminal Division should continue to investigate cyber intrusions within their criminal jurisdictions.
- **DHS should continue to enhance its network defense capabilities and information sharing initiatives but must increase its utilization and reliance on the deterrent effect of USSS cyber criminal investigations as an integral part of the department's cyber security efforts**. Although, as indicated within this thesis, defensive technology can never be expected to thwart the most determined or advanced attackers, defensive technology does provide a high level of protection. As presented within the thesis, in recognition of the inherent vulnerabilities in cyber systems, deterrent law enforcement operations are necessary to ensure attackers are identified and apprehended.

In closing, the thesis identifies additional areas of research that are required to support the development of adaptable policies scalable to the rapidly changing cyber threat environment. As demonstrated through the literature review, the existing research into the threats against U.S. critical cyber infrastructure has generally focused on the two key methods of attaining cyber security: 1) utilizing defensive technology as described in John McHugh, Alan Christie, and Julia Allen's article "Defending Yourself: The Role of

Intrusion Detection Systems," regarding intrusion detection systems,[7] for example, and 2) offensive operations that identify and eliminate the actors who seek to target our cyber systems[8] as discussed in Susan Brenner's article in the *Journal of Criminal Law and Criminology* titled "At Light Speed."

Areas for future research include a review of emerging technologies that provide more adaptable defensive precautions through leveraging artificial intelligence. At some point, it is possible that the technology will supplant the need for human decisions and intervention that is often identified as the point of failure during a post-intrusion review. Another area of valuable research is a review of successful cyber security efforts initiated by the private sector, how the need for those efforts was advertised within the corporate structure to gather support, and the way that those successes could be imitated or initiated throughout the government enterprise. Related to this topic, a comprehensive study of the cyber security efforts of other nations and whether those efforts could be employed within the U.S. could prove beneficial to policy makers. Finally, additional research regarding deterrence or game theory as it applies to low-level attackers, advanced/organized criminal actors, and nation-state supported cyber threats should be conducted to more thoroughly evaluate the effectiveness of offensive operations against attackers of different skill levels and motivations.

[7] John McHugh, Alan Christie, and Julia Allen, "Defending Yourself: The Role of Intrusion Detection Systems," *IEEE Software*, September 2000, 42.

[8] Susan W. Brenner, " 'At Light Speed': Attribution and Response to Cybercrime/Terrorism/Warfare," *Journal of Criminal Law and Criminology (1973-)* 97, no. 2 (January 1, 2007): 379–475, doi:10.2307/40042831.

ACKNOWLEDGMENTS

When I was accepted into the Naval Postgraduate School CHDS program, I expected to be challenged academically, professionally, and personally. What I had less appreciation for was the amount of support I would require from my professional colleagues, academic advisors, fellow students, and most importantly, my family.

My professional colleagues at the Secret Service's Criminal Investigative Division receive my thanks for allowing me to concentrate on this goal by picking up the workload when I was at the quarterly in-residence sessions. They were also called upon numerous times to serve as sounding boards for the innumerable papers and, of course, this thesis. For their support, I am deeply indebted.

To my fellow students of Cohort 1303/1304, I thank you for allowing me to benefit from your collective experiences in the Homeland Security enterprise and the camaraderie we developed while studying this critical shared mission in which we independently are not nearly as powerful. Through many late night "welfare checks" and commiseration, we benefitted from this shared experience, and I thank you for supporting me when the workload seemed insurmountable.

Thank you to all of the world-class NPS staff. The depth of professional experience of the CHDS instructors consistently reminded me that my understanding of the Homeland Defense and Security enterprise would be irrevocably broadened through this process. Among the staff, my greatest thanks are reserved for my thesis advisors, Drs. Kathleen Kiernan and Lauren Fernandez, without whom this thesis would still be incomprehensible musings on paper. They somehow kept me on track and supported me when in doubt and provided confidence and vision when I needed it most.

Finally, my deepest love and appreciation are reserved for my family: Cheryl, Kyra and Conner. Cheryl is undoubtedly the strongest part of this family and never fails to provide the spark to jumpstart me when I falter. Her strength of character and family coordination skills kept me in the game when pressures got too high and sleep was a rare privilege. Kyra and Conner fully supported my educational pursuit even as they prepared

to progress and succeed academically themselves. Perhaps most importantly, they recognized the thesis writing mania when it took hold and knew to steer clear. I owe this, and all of “my” accomplishments, to the team that is my family. Without your unwavering support, I could not have completed this effort. I love you all more than I can say.

I. FRAMING THE SCOPE

A. PROBLEM STATEMENT

Following the terrorist attacks of September 11, 2001, the U.S. government worked to reassure the American public and provide for their safety from terrorist attack. During this turbulent time, sweeping organizational changes were made to the government's structure to facilitate increased security and operational efficiency. Among the most significant was the creation of the Department of Homeland Security (DHS) with the passage of Public Law 107–296 (Homeland Security Act of 2002) on November 25, 2002.[1]

In 2001, the U.S. Secret Service (USSS) was operationally aligned within the U.S. Treasury Department where, since its formation in 1865 to suppress the counterfeiting of U.S. currency, it had continued to develop its expertise and experience consistent success in financial crimes investigations.[2] Over the course of its history, the Secret Service's investigative authorities had evolved, and the agency had adapted its capabilities to account for changing technologies that threatened the nation's critical financial infrastructure. As the financial sector became increasingly reliant on cyber technologies, and the threat emanating from cyberspace became more pervasive, the USSS consistently increased its investment in cyber-investigative capabilities. The USA Patriot Act, passed on October 26, 2001, called for an expansion of the USSS Electronic Crime Task Force (ECTF) model, which had been proven to be a successful method of investigating the terrorist use of cyber technologies and the prevention of attacks against the nation's financial infrastructure through aggressive enforcement and information sharing.[3]

In 2003, the USSS, although mandated to remain a distinct agency operating within its own authorities, was transferred to the Department of Homeland Security

[1] An Act to Establish the Department of Homeland Security and for Other Purposes (Homeland Security Act) Act of 2002, Pub. L. No. 107-296 Stat. 2135 (2002).

[2] Richard Harlow, "Two Missions, One Secret Service: The Value of the Investigative Mission" (master's thesis, Naval Postgraduate School, 2011).

[3] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

(DHS), whose mission was to ensure the security of the nation from terrorist attack.[4] Since that time, DHS's mission has expanded to include the security and resilience of the nation's 16 Critical Infrastructure and Key Resources (CIKR), which includes the financial infrastructure and cyberspace.[5] The National Protection and Programs Directorate (NPPD) was formed to coordinate the department's cyber-security mission but, as reflected in governmental reports, the directorate has underutilized DHS component cyber-investigative capabilities, namely the USSS cyber investigation expertise, to further the department's cyber-security mission.[6] This underutilization arguably affects the overall effectiveness and efficiency of the department.

Since 9/11, government agencies, predominantly representing the intelligence community (IC) and military cyber-attack units, have aggressively promoted the belief that any cyber threat targeting our nation's critical infrastructure should be designated as a "national security" threat, regardless of the motivations or identity of the attacker.[7] Not surprisingly, those proponents have also argued that they alone possess the requisite capabilities to successfully counter this existential threat to our national security through domestic and international cyber operations. Detractors have argued that domestic IC and military operations violate prohibitions that are in place to protect our citizens' privacy and civil liberties.

It is important to examine and better understand the cyber threats targeting our nation's critical infrastructure, as well as the motivations of the actual attackers, to facilitate the development and implementation of a comprehensive cyber security strategy for the government and private sector infrastructure owners. Once the threat has been accurately defined, agencies involved in cyber defense, cyber attack, intelligence or cyber law enforcement operations can be provided clear operational parameters and missions. A

---

[4] Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002).

[5] U.S. Department of Homeland Security (DHS), *National Infrastructure Protection Plan*, (Washington, DC: DHS, 2009) https://www.dhs.gov/national-infrastructure-protection-plan.

[6] Frank Deffer, *Planning, Management, and Systems Issues Hinder DHS' Efforts to Protect Cyberspace and the Nation's Cyber Infrastructure*, Office of the Inspector General (DHS-OIG, June 2011), https://www.hsdl.org/?view&did=683172.

[7] Thomas Rid, "The Great Cyberscare: Why the Pentagon Is Razzmatazzing You about Those Big Bad Chinese Hackers," *Foreign Policy*, March 13, 2013.

government-wide strategy, which leverages agency specific capabilities, can then be developed to ensure our cyber-security enterprise is optimally utilized. This strategy must include detailed policy guidelines for the government agencies involved in the effort as well as clear responsibilities for both the private and public sector in this collaborative effort. This research offers comparative information to support the formulation of government cyber-security policy that develops the most effective, integrated cyber-security methods while protecting our citizens' civil liberties and privacy.

B. BACKGROUND

1. Post-9/11 U.S. Government Terrorism Focus

With his 2002 State of the Union Address following shortly after the worst terrorist attack in our nation's history, President Bush began what is often described as one of the greatest transformations of American government policy and focus in our history.

> Our first priority must always be the security of our Nation, and that will be reflected in the budget I send to Congress. My budget supports three great goals for America: We will win this war; we'll protect our homeland and we will revive our economy….Time and distance from the events of September the 11th will not make us safer unless we act on its lessons. America is no longer protected by vast oceans. We are protected from attack only by vigorous action abroad, and increased vigilance at home.[8]

For many Americans, our recollection of personal and historical events are separated into "pre" and "post" September 11th time references. Enders and Sandler, in their study titled "After 9/11; Is it all Different Now?" state that President Bush's 2002 State of the Union Address strongly suggested that everything about American life changed on 9/11 and that the nation had to concentrate all its resources to fight a network of terrorists bent on committing violent acts against the homeland.[9] A historical review of the changes this country has undergone since 9/11 seem to bear out President Bush's

---

[8] George W. Bush, "2002 State of the Union Address," *Business Source Complete*, Vital Speeches of the Day, 68, no. 9 (February 15, 2002): 5.

[9] Walter Enders and Todd Sandler, "After 9/11: Is It All Different Now?" *Journal of Conflict Resolution* 49, no. 2 (April 1, 2005): 259, doi:10.1177/0022002704272864.

prediction. The nation's focus on defeating the terrorist threat and ensuring the greatest level of homeland security caused massive increases in expenditures to defeat the "new" threat.[10]

In the days immediately following the attacks of 9/11, the Bush administration sought to establish a framework to guide and codify the changes that he had indicated were neccesary in his address. These early decisions and efforts ushered in an era of sweeping organizational change to the government, including a reorganization of the U.S. intelligence program and the formation of a massive new cabinet level department. As these changes were initiated, the American public,which was struggling to regain its equilibrium from the attacks, was becoming much more accepting of increased government impact on citizens' privacy to defeat the perceived threat specifically focused on terrorism.

To quickly facilitate the steps the administration desired, on October 8, 2001, President Bush issued Executive Order (EO) 13228. This established an Office of Homeland Security within the Executive Office of the President (EOP) to be managed by an Assistant to the President for Homeland Security.[11] The primary mission of the new position was to develop and coordinate a comprehensive national strategy to secure the nation from *terrorist threat or attack.*[12] In developing the national strategy, the new position required the authority to coordinate with many entities from both inside and outside the government. The responsibilities and duties of this office also included managing the collection and analysis of information regarding *terrorist groups* within the United States, coordination and information sharing with the intelligence community, preparedness and mitigation of *terrorist attacks* within the homeland, prevention of future *terrorist* attacks through information sharing, response and recovery to *terrorist attacks*,

---

[10] Ibid.

[11] George W. Bush, "Executive Order Establishing Office of Homeland Security," in *Proceedings of the 12th Annual Conference on Computers, Freedom and Privacy* (New York: ACM, 2002), http://dl.acm.org/citation.cfm?id=543487.

[12] Ibid., 1.

incidence management, and to ensure continuity of government in the face of *terrorist attacks.*[13]

In what is commonly accepted as the most impactful and debated legislative action of the post-9/11 era, on October 26, 2001, the 107th Congress passed Public Law 107–56 titled "The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001.[14] (hereinafter "the Patriot Act"). This legislation was specifically directed at providing increased authorities and capabilities to government agencies to more effectively investigate, identify and interupt the terrorist threat to the homeland. To support the counter-terrorism focus of the government in the post-9/11 era, new techniques included "enhanced" surveillance procedures which involved sweeping changes to many provisions of the Foreign Intelligence Surveillance Act (FISA) of 1978, strengthened laws regarding terrorist financing, border security, intelligence sharing amongst law enforcement and the intelligence community; and changes to the bank secrecy laws.'[15][16] Consistent with the effort to identify and interupt terrorist activities, the Patriot Act also commanded the U.S. Secret Service to expand its network of ECTFs with investigative emphasis being placed on electronically enabled crimes which were supporting terrorism funding or operations.[17]

Shortly therafter, on October 29, 2001, President Bush issued Homeland Security Presidential Directive-1 (HSPD-1), which formed the Homeland Security Council (HSC) to assist the new Assistant to the President in securing the homeland from the threat of future terrorist attacks.[18] The HSC was directed to be composed of senior executives

---

[13] Ibid., 2.

[14] USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[15] Ibid.

[16] Paul T. Jaeger, John Carlo Bertot, and Charles R. McClure, "The Impact of the USA Patriot Act on Collection and Analysis of Personal Information under the Foreign Intelligence Surveillance Act," *Government Information Quarterly* 20, no. 3 (July 2003): 295, doi:10.1016/S0740-624X(03)00057-1.

[17] USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[18] George Bush, "Homeland Security Presidential Directive 1: Organization and Operation of the Homeland Security Council" *Weekly Compilation of Presidential Documents,* November 5, 2001, https://www.hsdl.org/?view&did=1132.

from select Cabinet-level government agencies who could provide guidance to the administration on protecting the homeland and responding to the terrorist threat.

A review of the government response to the 9/11 attacks and the intiatives that were undertaken underscores that the government was wholly focused on the terrorist threat to the homeland from foreign actors with little initial focus on catalogueing potential terrorist targets within the homeland or any real understanding of the threat to the safety and security of the homeland and American population. The next section identifies and documents the government's increasing realization that terrorism was only one of many threats facing the homeland, and that a much larger organization which could prepare and plan for a wider range of the threats, was required.

2. Department of Homeland Security and the Government's Changing Focus

On November 25, 2002, the 107th Congress passed Public Law 107–296, commonly identified by the short title "The Homeland Security Act of 2002" (HSA).[19] The HSA formed the Department of Homeland Security (DHS), with the authority to operate as an executive department of the United States.[20] The primary mission of the department was to prevent terrorist attacks, lessen the nation's vulnerability to terrorist attack, minimize damage from attacks, and increase the national resiliency.[21] Recognizing that many existing government agencies possessed homeland security related capabilities and authorities, the Act also identified agencies that were eventually organizationally re-aligned under the new department, while also forming new component agencies through the combination of multiple agencies or missions under one component agency.

Although the impetus for the formation of DHS was specifically in response to the perceived terrorist threat, the inclusion of the Federal Emergency Management Agency (FEMA), which was the recognized authority in responding to mass casualty or

---

[19] Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002).

[20] Ibid.

[21] Ibid.

resiliency events, unwittingly provided a wider prism through which to view the homeland security mission.[22] This wider mission space offered the new department opportunities that would enable it to quickly grow its influence beyond terrorist attack prevention, response, and mitigation, and move aggressively into an "all hazards" approach to homeland security.[23] According to some researchers, this "all hazards" approach has resulted in some DHS agencies being forced to de-emphasize their legacy missions to fulfill the new requirements of the department.[24]

Among the 22 agencies re-aligned under the newly formed department were the U.S. Secret Service and the U.S. Coast Guard, two agencies that struggled to retain their identities and unique history while still adding value to the new department. For the U.S. Secret Service, which had been a valued agency of the U.S. Treasury Department since its formation in 1865, re-alignment to a department that had limited interest in financial crime investigations and dignitary protection was tumultuous. Unrecognized by many within the Secret Service during those early years in DHS, portions of the department's changing focus could allow the Secret Service to position itself and its cyber capabilities and authorities at the forefront of the growing departmental mission of cyber crimes and cyber security operations.

Although, as discussed above, the DHS's initial focus on terrorism-related matters and its increasing gravitation toward an "all hazards" approach to homeland security is often identified as "mission creep," the research supporting this thesis identified that the U.S. government had been steadily moving toward an "all hazards" approach since the 1990s. Increasingly, the government had been gaining better understanding of the interconnectivity and vulnerability of the nation's identified critical infrastructures to terrorist attack or other disruption.

---

[22] Dara Kay Cohen, Mariano-Florentino Cuéllar, and Barry R. Weingast, "Crisis Bureaucracy: Homeland Security and the Political Design of Legal Mandates," *Stanford Law Review* 59, no. 3 (December 1, 2006): 26, doi:10.2307/40040307.

[23] Ibid., 26.

[24] Ibid., 27.

In 1996, President Clinton established the President's Commission of Critical Infrastructure Protection (PCCIP) with the mission of providing guidance regarding the scope and nature of the threat and vulnerabilities of the nation's critical infrastructure with a specific focus on threats emanating from cyber space.[25] The commission identified critical infrastructures, grouped in "sectors," the loss or disruption of which could debilitate or destroy the nation's defense, stability or economic well-being.[26] It also identified infrastructure that included power, communications, emergency services, water, transportation, and banking/financial systems among others.[27] Although the commission found that there were no imminent human-caused threats that could result in a national crisis, it did identify that the threat from terrorism or attack, specifically through cyber attack was a growing threat that required attention from the government.[28]

In response to the commission's findings, in May 1998, President Clinton issued classified Presidential Decision Directive-63 (PDD-63) that called for "reliable, interconnected, and secure information system infrastructure by the year 2003; and significantly increased security to government systems by the year 2000."[29] PDD-63 also called for an immediate establishment of a national center to warn of and respond to attacks, and to ensure the capability to protect critical infrastructures from intentional acts by 2003.[30] Finally, the document directed the administration to addresses the cyber and physical infrastructure vulnerabilities of the federal government by requiring each department and agency to work to reduce its exposure to new threats.[31]

---

[25] John Moteff, *Critical Infrastructures: Background, Policy, and Implementation* (CRS Report RL30153) (Washington, DC: Congressional Research Service, February 21, 2014), 6.

[26] President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (Washington, DC: President's Commission on Infrastructure Protection, October 1997), 19.

[27] Ibid., 20.

[28] Ibid.,14.

[29] William Clinton Administration, *Presidential Decision Directive-63* (Washington, DC: The White House, May 22, 1998), http://fas. org/irp/offdocs/pdd/pdd-63. htm.

[30] Ibid.

[31] Ibid.

DHS is uniquely suited to this mission when one considers the pre-existing government concentration on critical infrastructures and the varied expertise represented within DHS component agencies. Component agencies, including the Secret Service, FEMA, and others already possessed comprehensive legal authorities and capabilities that provided DHS with the immediate authority and expertise to secure the homeland and our cyber supported Critical Infrastructure and Key Resources from attack.

C. RESEARCH QUESTIONS

The frequency, severity, and effects of attacks emanating from cyberspace that target U.S. critical infrastructure and interests continue to increase. As the lead U.S. government agency mandated to coordinate the security of the nation's cyber-supported critical infrastructure, DHS seeks to identify and implement the most effective methods to enhance American cyber security. To achieve success in this developing homeland security mission, DHS's coordination efforts must leverage defensive technology, the offensive and cyber-intelligence collection capabilities of the NSA/DOD and FBI, and the deterrent effect offered by cyber law enforcement activities.

- **Primary research question:** What strategies can the U.S. government develop that support the efforts of DHS, in concert with other governmental cyber security entities, to ensure the nation's cyber-supported critical infrastructure is provided with the most comprehensive security, while ensuring our citizens' privacy and security are preserved?
- **Secondary research question:** How could the application of established law enforcement investigative authorities and capabilities augment the technology-centric, defensive cyber methods currently utilized by the Department of Homeland Security to secure the nation's critical infrastructure against criminal cyber intrusions?

D. RESEARCH METHOD

Through the application of policy analysis, this thesis examines the cyber-security mission, authorities and capabilities of four components: the Department of Homeland Security, the National Security Agency (NSA) (inclusive of the Department of Defense's Cyber Command), the Federal Bureau of Investigation (FBI) and the U.S. Secret Service. The thesis features a comparison of the applicability and effectiveness of those agency's specific cyber authorities and capabilities. These agencies were chosen for this thesis

because DHS was mandated to coordinate the homeland security effort, the NSA is the leading IC cyber security and attack agency and the FBI and USSS share concurrent jurisdiction regarding the investigation of cyber intrusions against any protected computer system.

The inquiry reviews departmental cyber-security policies and compares the effectiveness of the department's technology-centric cyber security approach against the deterrent effect realized through offensive, specifically law enforcement, cyber operations. Cyber-law enforcement effectiveness is also contrasted against the suitability and effectiveness of the militarization of cyberspace and the cyber-security mission.

The thesis is limited to a review of DHS's efficiency and success in the cyber-security mission, the statutory cyber-investigative authorities and capabilities of the USSS and the FBI, and the suitability of the current cyber-security methods that predominantly feature defensive technology. In line with this avenue of analysis, the review examines the suitability and effectiveness of the DOD/NSA's position as the primary security apparatus defending the nation's cyber-supported critical infrastructure. Because scientifically quantifying the deterrent effect of offensive cyber operations requires the accurate measurement of its effect on the personal beliefs and activities of a prospective attacker, this product does not attempt to capture the numbers. Instead, the research analyzes the available literature on deterrence to a prospective cyber intruder that results from offensive cyber-security effort. Given the numerous drivers that cause a malicious cyber actor to intrude into a protected cyber system, accurately accounting for a comprehensive deterrent effect may be impossible or lead to offering inaccurate observations.

The source data includes academic and governmental sources. These sources include governmental regulatory publications, existing statuary regulation and laws, scholarly products that directly relate to thesis topics, and program reviews of various cyber-security missions and capabilities. To control bias in the supporting research, the collection of information included a diverse cross section of practitioners; the research does not include interviews or surveys.

At the conclusion of this thesis, a more comprehensive understanding of the U.S. government's cyber-security policies and the successes or limitations of those policies is made clear. Additionally, a greater understanding of the efficiency and effectiveness of cyber-security practices, the legal implications and privacy concerns inherent in the current militarization of cyberspace and the effectiveness of cyber-law enforcement activities is gained. This thesis allows the reader to apply the knowledge to propose policies to support a future, comprehensive cyber-security effort while still protecting the Internet's openness and functionality.

E. CHAPTER OVERVIEW

Chapter II documents and discusses the executive orders, presidential directives, and legislation that propelled the changing cyber security mission of the government, specifically through the Department of Homeland Security, in its mission of safeguarding the critical infrastructure from attack and exploitation. Chapter II provides the reader with the current government cyber security policy and provides a basis to understand how the development of cyber security policies evolved to its current state.

Chapter III provides the literature review that summarizes the existing knowledge and identifies opportunities for further research within the subject area. The review includes sources representing government, academia, and the private sector. Additionally, applicable government laws and policies, as well as agencies responsible for the cyber security of the nation's critical infrastructure are reviewed and analyzed to capture the opinions of the leading experts regarding the effectiveness and complimentary utilization of the two principal approaches to cyber security. These approaches are 1) the defensive use of technology and 2) offensive operations, which provide a deterrent effect.

Chapter IV provides a description of the evolving cyber security missions of DHS, the National Security Agency (NSA) inclusive of the Department of Defense (DOD)/Cyber Command, The Federal Bureau of Investigation (FBI) and the U.S. Secret Service.

Chapter V applies the evidence from the literature review to analyze the implications of the current cyber-security strategies including: defensive techniques, the

application of military offensive cyber attack and exploitation techniques, national security centric investigations, and the application of criminal investigations and prosecution to deter cyber attacks against the nation's critical infrastructure.

Finally, Chapter VI offers conclusions, policy recommendations, and areas of future research to support development of a comprehensive cyber security strategy for this nation.

II. POST-9/11 U.S. GOVERNMENT CIKR CYBER FOCUS

The preceding chapter chronicled the sweeping changes that the terror attacks of September 11, 2001, brought to America and its people. In the years immediately following the attacks, the government worked to develop a framework of governance and organization to support a comprehensive homeland security enterprise in an effort to secure the nation from the threat of terrorism. The formation of the Department of Homeland Security, in combination with sweeping new legislation, helped identify, disrupt, and in some cases, prosecute, terrorist plots against the homeland. But, as DHS developed its methods on securing the nation's CIKR from terrorist attack, the U.S. government was moving toward a greater understanding of the threats emanating from cyberspace and issuing guidance and legislation to secure this new area from cyber attacks.

A. PRESIDENTIAL CYBER POLICY DIRECTIVES AND CYBER EXECUTIVE ORDERS

Although the post-September 11 government focus was predominately on preventing another act of terrorism, in February 2003, President George Bush issued the "National Strategy to Secure Cyberspace" in recognition of the increasing importance that cyber supported critical infrastructures played in our nation's security.[32] This strategy called for a national effort to prevent future cyber attacks, reduce vulnerabilities and increase the resilience of our nation's critical systems.[33] Additionally, the strategy initiated the often-repeated statement that the majority of the nation's critical infrastructure is owned by the private sector, and that private organizations naturally possess a much greater capacity for enhancing our cyber security.[34] This early strategy also identified that attributing a cyber attack to a particular threat actor is the most difficult, but most important, aspect of responding to cyber attacks. In recognition of this,

---

[32] *The White House, National Strategy to Secure Cyberspace* (Washington, DC: White House Office, February 2003), https://www.hsdl.org/?view&did=1040.

[33] Ibid., 9.

[34] Ibid., 10.

the president called for increased information sharing with the private sector, additional support for law enforcement operations in responding to attacks against the private sector, and more advanced responses from the intelligence community in responding to national security events targeting secure government systems.'[3536]

Shortly after issuing the above strategy, on December 17, 2003, President Bush announced the release of Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection (HSPD-7).[37] HSPD-7 formalized the national policy regarding securing the nation's critical infrastructure and cyber systems from terrorist attack or exploitation.[38] With this directive, DHS, which had been formed to secure the homeland from terrorist attacks, saw its mission officially expanded to include "all hazards" critical infrastructure protection with an emphasis on securing our nation's cyber supported critical infrastructure. Finally, this directive continued with the warning that DHS must ensure the privacy of American citizens' information and communications while enhancing cyber security.[39]

In January 2008, President Bush launched the Comprehensive National Cyber Security Initiative (CNCI), which supported mandates reportedly issued in the classified National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD54/HSPD23).[40] In an effort to increase the government's cyber security effectiveness and operations, the CNCI mandated increased government investment in cyber security monitoring tools, training, and increased information-sharing operations with the private sector but provided little funding or support for cyber investigative

---

[35] Ibid., 12.

[36] Ibid., 13.

[37] George W. Bush Administration, *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection* (Washington, DC: White House Office, December 17, 2003).

[38] Ibid.

[39] Ibid.

[40] John Rollins and Anna Henning, *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations* (CRS Report No. R40427) (Washington DC: Congressional Research Service, March 10, 2009), 2.

operations.[41] Of note, the CNCI specifically designated DHS as the lead for coordinating with the private sector to secure the nation's CIKR from cyber attack.[42]

In an effort to keep the government focused on the threat emanating from cyberspace during the election cycle, in December 2008, the Center for Strategic and International Studies released their report titled "Securing CyberSpace for the 44th Presidency."[43] This report called on the president to designate cyberspace as a vital asset of the nation and to use all assets at his disposal, including diplomacy, the military, economic prosperity, and law enforcement to ensure that cyberspace remains available to all citizens and businesses while ensuring their privacy.[44] Although this report identified nation state actors as the most damaging of the threats the nation faced, the report spent considerable time enumerating the threat posed by cybercrime and the need to develop cooperative international standards to quickly and effectively respond to criminal cyber attacks.[45] In fact, the report noted that successful law enforcement actions result in attacker attribution, more comprehensive repair, and the most effective level of deterrence because "the criminal hacker community pays attention when other criminal computer criminals are caught and punished."[46] In effect, a successful cyber intrusion investigation and apprehension of those responsible results in a deterrent effect beyond the attackers who are brought to justice, the deterrence of attacks by prospective intruders may also be realized.

Indicative of the government's focus on cyber security and the threats to the nation's critical infrastructure, shortly after taking office, President Barack Obama's National Security Council (NSC) release the Cyberspace Policy Review.[47] In a first-of-

---

41 National Security Council (NSC), *Cyberspace Policy Review: Securing America's Digital Future* (New York: Cosmo Reports., May 2009).

42 "The Comprehensive National Cybersecurity Initiative," The White House, accessed September 26, 2014, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

43 James A. Lewis, *Securing Cyberspace for the 44th Presidency* (Washington, DC: Center for Strategic and International Studies, December 2008).

44 Ibid., 13.

45 Ibid., 28.

46 Ibid., 37.

47 NSC, *Cyberspace Policy Review*.

its-kind declaration, the review identified cybercrime committed by both state and non-state actors as a growing threat that need to be accounted for in any cyber security program.'[48][49] Additionally, the review highlighted the financial loss being experienced by our nation's financial institutions from cybercrime as a national priority, called for the establishment of a "cyber czar" to coordinate the national effort, and designated cyber as one of the administration's key priorities.[50]

In March 2011, the administration followed those directives with Presidential Policy Directive-8 (PPD-8), which established a mandate to develop a process to systematically secure the nation's cyber supported critical infrastructure and to ensure an effective response and recovery plan from all hazards.[51] Once again, the administration identified the Secretary of DHS as the coordinator for this effort.[52]

Of particular importance, in October 2012, President Obama issued PPD-20 (classified) which was discussed in a *Washington Post* article on November 12, 2012.[53] According to media reports, PPD-20 provided strict but broad guidance for federal agencies and the military to operate both offensively and defensively in cyberspace or in furtherance of the prosecution of the, as yet undefined, cyberwar or cyber terrorism.[54] Also, as reported by the *Washington Post*, the directive explicitly delineated between cyber defense (operations conducted within one's own network) and cyber operations (actions outside of one's own network).[55] Although the directive specifically highlighted

---

[48] Ibid., 3.

[49] Ibid., 5.

[50] Ibid., 8.

[51] "Presidential Policy Directive 8: National Preparedness," The White House, March 30, 2011, https://www.hsdl.org/?view&did=7423.

[52] Ibid., 4.

[53] Barak Obama Administration, *Presidential Policy Directive 20: Cyber Operations of Military and Federal Agencies (Classified*) (Washington, DC: White House Office, October 2010), https://www.hsdl.org/?view&did=725668; Ellen Nakashima, "Obama Signs Secret Directive to Help Thwart Cyberattacks," *Washington Post*, November 14, 2012, http://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html.

[54] Nakashima, "Obama Signs Secret Directive

[55] Ibid.

the requirement that our citizens' privacy must always be protected in offensive operations and that law enforcement action should always be the primary response to cyber attack, the *Post* article indicates that General Keith Alexander of the National Security Agency (NSA) argued for less restrictions being placed on his Department of Defense (DOD) cyber attack forces.[56]

On February 12, 2013, President Obama issued PPD-21, to codify the government's policy on ensuring the security and resilience of the nation's critical infrastructure.[57] This policy required the DHS secretary to work with state, local and tribal partners to identify the nation's interconnected critical infrastructures; conduct security assessments through the utilization of DHS component agency's authorities; and to work with the Attorney General to investigate and prosecute physical and cyber attacks against the infrastructure.[58]

Finally, on February 19, 2013, the Obama administration issued Executive Order 13636 (EO-13636)—Improving Critical Infrastructure Cyber Security. This EO directed the DHS secretary to develop a cyber-security framework that provides specific guidance to private infrastructure owners in securing their systems while maintaining the privacy of system owners and users.[59] This EO also directed the secretary to initiate a program to provide classified information to system owners in an effort to provide actionable information to be utilized in the cyber security effort.[60]

B. DHS CYBER POLICIES AND CHANGING MISSION FOCUS

By 2005, the department's single issue focus centering on terrorism was being replaced by a focus on an "all hazards" approach to safeguarding the identified Critical Infrastructure and Key Resources (CIKR) that form the underpinnings of the nation's

---

56 Ibid.

57 "Presidential Policy Directive 21: Critical Infrastructure Security and Resilience," The White House, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

58 Ibid.

59 Exec. Order 13636, C.F.R. 11739 (2013).

60 Ibid.

prosperity.[61] During his July 13, 2005, speech announcing his "Second Stage Review" of the department's goals and organization, DHS Secretary Chertoff indicated that the department was focusing on the nation's CIKR. Additionally, with his announcement of a new Assistant Secretary for Cyber and Telecommunications Security within the department, Secretary Chertoff brought cyber security and the cyber systems that support the CIKR into the forefront of the DHS mission.[62]

In 2008, Secretary Chertoff issued the DHS Strategic Plan for 2008–2013, which was envisioned to set the five-year organizational priorities for the department.[63] Although by this time, most administration strategy documents were increasingly focused on cyber security and the interconnected critical infrastructures, this publication focused on an "all hazards" approach with specific sections on border security, immigration, importation of dangerous goods, and critical infrastructure that was vulnerable to cyber attack.[64]

The National Infrastructure Protection Plan (NIPP) quickly followed the Strategic plan in 2009.[65] The NIPP clearly identified that cyber attack had the capability to affect all of the nation's CIKR due to the interconnectivity afforded by the Internet and that the threat was an expected to constantly increasing.[66] Although the NIPP spent considerable time enumerating the authorities of DHS to secure the nation's infrastructure through defensive measures, none of the various component agencies of the department, including DHS, law enforcement agencies nor their legal authorities, were referenced in the document. In fact, the only law enforcement entity referenced was DHS' shared responsibility with the Department of Justice (DOJ), through the Federal Bureau of

---

61 "Secretary Michael Chertoff, U.S. Department of Homeland Security Second Stage Review Remarks," U.S. Department of Homeland Security, July 13, 2005, http://www.dhs.gov/xnews/speeches/speech_0255.shtm.

62 Ibid.

63 U.S. Department of Homeland Security (DHS), *One Team, One Mission, Securing Our Homeland: U.S. Department of Homeland Security Strategic Plan, Fiscal Years 2008–2013* (Washington, DC: DHS, 2008), http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA487194.

64 Ibid., 6–15.

65 DHS, *National Infrastructure Protection Plan*.

66 Ibid., 12.

Investigation (FBI).[67] As will be discussed later in this thesis, DHS' focus on defensive cybersecurity measures, and the almost total dismissal of DHS' own law enforcement agency's authorities and capabilities, became a common issue in the future operations.

In February 2010, DHS, now headed by the newly confirmed Secretary Janet Napolitano, issued the first *Quadrennial Homeland Security Review* (*QHSR*), which was envisioned to outline a framework to guide homeland security participants toward a common goal.[68] Specifically, the *QHSR* identified that a safe and secure homeland required more than preventing terrorist attacks, it also identified that citizens' privacy must be secured while protecting the nation's economic security and way of life.[69] The *QHSR* continued to stress an "all hazards" approach to homeland security but also maintained that the threat from transnational organized crime groups, including cyber crime groups, posed to the homeland was a growing issue requiring the nation's attention.[70] For the first time, cyber crime and attack was listed as the third gravest threat to our nation's prosperity, behind only weapons of mass destruction (WMD) and global violent extremism, although, once again, DHS chose to concentrate on defensive technology.[71]

Five months later, in July 2010, DHS released the *Bottom-Up Review* (*BUR*), which sought to examine the programs, plans, and structures of the department and to align the organizational structure and programmatic activities with the *QHSR*.[72] The *BUR* was the first departmental policy document to specifically highlight the U.S. Secret Service (USSS) and Immigrations and Customs Enforcement's (ICE) criminal cyber investigative capabilities although the document also identified the department's National Protection and Programs Directorate (NPPD) as coordinating the department's cyber

---

67 Ibid., 20.

68 U.S. Department of Homeland Security (DHS), *Quadrennial Homeland Security Review* (Washington, DC: DHS, February 2010, http://www.dhs.gov/quadrennial-homeland-security-review-qhsr.

69 Ibid., 9.

70 Ibid., 14.

71 Ibid., 19.

72 U.S. Department of Homeland Security (DHS), *Bottom-Up Review* (Washington, DC: DHS, July 2010), http://www.dhs.gov/bottom-review.

security activities.[73] Later, in a section specifically outlining the department's cyber security mission and capabilities, the review recognized that the USSS possessed the legal authorities to prevent, detect, and investigate cyber financial crimes while working closely with state and local law enforcement to secure our nation's cyber supported critical infrastructure.[74]

In contrast to the *BUR*, in September 2010, a DHS cyber security information webpage, titled "Preventing and Defending against Cyber Attacks," listed the department's cyber security mission areas. The operations promoted in this document included automated intrusion detection systems (IDS), secure identity management tools, information sharing programs, privacy protection tools, and workforce development initiatives with no mention of the department's own cyber law enforcement agencies.[75]

The department's shifting focus towards the importance of cyberspace was complete when, in November 2011, DHS released its *Blueprint for a Secure Cyber Future*, which specifically outlined the cyber security strategy for the homeland security enterprise.[76] The blueprint's four goals for protecting cyber-supported critical infrastructure included; reduce exposure to cyber risk, ensure priority response and recovery, increased resilience and the ability to maintain situational awareness.[77] Although this document was also indicative of the department's focus on intrusion detection tools and technology, when law enforcement activities were described, the department chose to highlight the investigative activities of the FBI led National Cyber Investigative Joint Task Force (NCIJTF).[78]

The documents highlighted in this chapter identified the post-September 11 U.S. government's shifting terrorism-centric focus towards a focus on enhancing security

---

[73] Ibid., 21.

[74] Ibid., 37.

[75] "Preventing and Defending against Cyber Attacks," U.S. Department of Homeland Security, September 2010, http://www.dhs.gov/xlibrary/assets/preventing-and-defending-against-cyber-attacks.pdf.

[76] U.S. Department of Homeland Security (DHS), *Blueprint for a Secure Cyber Future* (Washington, DC: DHS, November 2011), http://www.dhs.gov/blueprint-secure-cyber-future.

[77] Ibid., 4.

[78] Ibid., 21.

and resilience to “all hazards” with special emphasis on the threat emanating from cyber space. Although DHS was formed to safeguard the nation from future terrorist attacks, the department was also slowly shifting to a cyber security and “all hazards” focus. As described in the PPDs, EOs and policy/strategy documents, and as will be discussed during later chapters regarding policy analysis, to some DHS component agencies, in spite of this shift, the department continued to emphasize building internal DHS capabilities, technology, and information sharing, and less willing to leverage DHS legacy agencies and their authorities. Chapter III reviews available literature pertaining to cyber-security tools, techniques and procedures and compares the effectiveness and applicability of defensive cyber-security tools against offensive activities. The offensive activities, and the deterrence that results from the application of these methods, will include cyber law enforcement activities and the use of the military, aka cyber attack, forces in cyberspace.

THIS PAGE INTENTIONALLY LEFT BLANK

III. LITERATURE REVIEW

The purpose of the literature review is to summarize the existing knowledge and identify opportunities for further research within the subject area. The review includes sources representing government, academia, and the private sector. Additionally, applicable government laws and policies, as well as the specific agencies responsible for the cyber security of the nation's critical infrastructure were reviewed and analyzed to capture the opinions of the leading experts regarding the two principal approaches to cyber security: 1) the defensive use of technology and 2) offensive operations, which provide a deterrent effect.

1. Defining the Mission

As was documented throughout the previous chapters, the government's mandate to DHS to secure the 16 identified CIKRs from attack and ensure their resiliency has an inherent friction that inhibits success, as most critical infrastructure is privately owned and existing government and private entities resist DHS' leadership and mandates.[79] In addition, all CIKRs are supported by, or dependent on, the nation's cyber infrastructure and technology and are vulnerable to threats emanating from cyberspace.[80] Throughout the department's attempts to secure cyberspace and the related infrastructures, private infrastructure owners and other government agencies have resisted the department's mandates and guidance as unlawful, ineffective, or a violation of privacy.[81] In a continuing effort to help DHS fulfill its mission, both the Bush and Obama administrations issued directives relating to cyber and critical infrastructure security.

79 U.S. Government Accountability Office (GAO), *DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise* (GAO-08-825) (Washington, DC: GAO, September 2008), https://www.hsdl.org/?view&did=235401.

80 DHS, *Bottom-Up Review.*

81 Matthew Fleming and Eric Goldstein, *An Analysis of the Primary Authorities Governing and Supporting the Efforts of the Department of Homeland Security to Secure the Cyberspace of the United States* (Arlington, VA: Homeland Security Studies and Analysis Institute, May 24, 2011), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2182675.

However, there is a lack of existing binding legal authorities to compel the compliance of the resistant entities.[82]

In 2003, President George W. Bush issued Homeland Security Presidential Directive (HSPD)-7, the Critical Infrastructure Identification, Prioritization, and Protection Act.[83] This directive assigned DHS the mission of coordinating the defense of our nation's critical infrastructure, mostly through information sharing and guidance to private owners. The defensive aspect of this directive may have resulted in DHS's perceived reliance on defensive technologies in fulfilling its cyber-security mission. Since that time, both the Bush and Obama Administrations have issued numerous cyber-security related directives including; the National Strategy to Secure Cyber Space,[84] the Comprehensive National Cyber Security Initiative,[85] the Cyber Space Policy Review,[86] and most recently, Executive Order (EO) 13636- Improving Critical Infrastructure Cyber Security,[87] and Presidential Policy Directive (PPD) 21 - Critical Infrastructure Security and Resilience.[88]

B. THE DEFENSIVE APPROACH TO CYBERSECURITY

These PPDs, EOs and federal laws have given DHS the mission of securing the nation and the resiliency of its sixteen critical infrastructure and key resources from terrorist attack and other disasters. Through a comprehensive review of such governmental guiding documents as the *Quadrennial Homeland Security Review* (*QHSR*),[89] the *Bottom-Up Review* (*BUR*),[90] and the *Blueprint for a Secure Cyber*

82 Ibid.

83 George W. Bush Administration, *Homeland Security Presidential Directive 7*.

84 White House, *National Strategy to Secure Cyberspace*.

85 "The Comprehensive National Cybersecurity Initiative."

86 NSC, *Cyberspace Policy Review*.

87 Exec. Order 13636, C.F.R. 11739 (2013).

88 "Presidential Policy Directive 21."

89 DHS, *Quadrennial Homeland Security Review*.

90 DHS, *Bottom-Up Review.*

Future.[91] DHS leadership clearly indicated that it believes that comprehensive cyber security is achieved through defensive technology.

Experts in cyber security argue that technology does have specific uses and can be an effective tool when utilized as part of a technique known as "defense in depth."[92] This technique, which deploys concentric "rings" of security, is actually an adaptation of a common technique used in physical security operations; as a potential attacker moves further into a protected system the security controls are increasingly stringent and subject to greater scrutiny. This technique results in the greatest security measures being applied to the most important aspects of a security operation and describes the technique used by the U.S. Secret Service in protecting the U.S. president. The technique is also supported by other experts in the cyber-security field who agree that a system of active defense is much more effective than a static (passive) defense.[93]

Other experts argue that the risks to national critical infrastructure far outweigh the nation's abilities to provide security through technological measures.[94] John McHugh, Alan Christie, and Julia Allen stress that, although the technology is still relatively immature and being constantly developed, an intrusion detection system (IDS), which is a static system, is effective at notifying system owners of an intrusion attempt on a timely basis and are not meant to thwart the attack.[95] Additionally, these systems are most effective when the IDS is protecting a defined goal—hardly a useful delineation in regards to DHS's mandate to protect all cyber-supported critical infrastructure, which is predominantly privately owned. Also, because a defined goal is required for these tools to work, Teodor Sommestad, Mathias Ekstedt, and Pontus Johnson stress that this ideal may

---

91 DHS, *Blueprint for a Secure Cyber Future*.

92 O. Sami Saydjari, "Cyber Defense: Art to Science," *Communications of the ACM* 47, no. 3 (March 2004): 52–57.

93 Ibid., 54.

94 Abraham D. Sofaer and Seymour E. Goodman, "Cyber Crime and Security. The Transnational Dimension," in *The Transnational Dimension of Cyber Crime and Terrorism*, eds. Abraham D. Sofaer and Seymour E. Goodman (Stanford, CA: Hoover Institution Press, 2001), http://media.hoover.org/documents/0817999825_1.pdf.

95 John McHugh, Alan Christie, and Julia Allen, "Defending Yourself: The Role of Intrusion Detection Systems," *IEEE Software*, September 2000, 42.

be unattainable because defenders can't be sure what the intruder will actually attack.[96] McHugh et al. have also pointed out that sophisticated attackers may direct their initial attack against the IDS to remove the security system, freeing them to move freely throughout the target system.[97]

To address the concern that the target of an undiscovered attack cannot be identified/known, DHS and supporting cyber-security entities have performed variety of techniques ranging from tabletop exercises to penetration testing ("pen testing") of the target systems. Although indications are that tabletop exercises can provide valuable insight for each of these tools, many examples of failure have resulted.

Since 2004, DHS has conducted three national level exercises, titled Cyberstorm (versions 1, 2 and 3), to test the effectiveness of partner collaboration, information sharing, and response to an identified attack.[98] Subsequent DHS after-action reports indicated that these exercises were very successful and greatly increased the nation's cyber security.[99] However, according to Sommestad et al., tabletop testing merely helps manage the response to intrusions but, because there is no assurance of the target and type of attack an adversary will choose, there is no assurance that the results are scientifically valid.[100] Additionally, Sommestad et al. indicate that penetration testing of targeted systems has been proven to be a valid method of recording when an attack was successful in exploiting a known vulnerability but that an unsuccessful pen test, conversely, does not indicate that a vulnerability is not present, just that the test did not seek to exploit an unidentified vulnerability.[101] Ross Anderson, in his "Paddy" scenario, adds that a cyber-system defender has to identify all vulnerabilities to achieve success,

---

96 Teodor Sommestad, Mathias Ekstedt, and Pontus Johnson, "Cyber Security Risks Assessment with Bayesian Defense Graphs and Architectural Models," in *42nd International Conference on System Sciences, 2009*, ed. Ralph H. Sprague Jr. (Piscataway, NJ: IEEE, 2009), 2, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4755419.

97 McHugh, Christie, and Allen, "Defending Yourself," 43.

98 GAO, *DHS Needs to Fully Address Lessons Learned*.

99 Ibid.

100 Sommestad, Ekstedt, and Johnson, "Cyber Security Risks Assessment," 9.

101 Ibid., 7.

but an attacker (Paddy) must only identify one vulnerability to achieve success.[102] In effect, the old adage commonly used in discussions related to sporting events that it is easier to attack than defend may prove true in the cyber realm.

Some experts, who concede that technology may provide added value as a defensive component to the nation's cyber-security precautions, argue that the voluntary use of technology will never be successful.[103] Mason Rice, Robert Miller, and Sujeet Shenoi point out that most infrastructures are privately owned and that proposed government mandates may be perceived as a violation of the basic rights of American citizens to be free from government intrusion into their private holdings.[104] In her article "Growing Threat," Valentina Pasquali proposes that the resistance to additional defensive cyber-security measures is not a result of a system owner's disbelief in the threat but instead is a lesson in economics. He indicates that defensive cyber-security tools are an additional cost to a business's bottom line and are not a revenue-generating tool.[105] Going further with this theme, Butler Lampson proposes that defensive security measures will not be embraced if they are inconvenient to use, cause a diminished operational system capacity (speed) or cost more than the system owner is willing to spend.[106]

In Ranjan Pal and Leana Golubchik's conference paper, "Analyzing Self-Defense Investments in Internet Security under Cyber-Insurance Coverage," the theory that a system of mandatory cyber-security measures modeled after a mandatory system of insurance, when deployed across the nation's public and private infrastructure, will

---

102 Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. (New York: Wiley, 2001).

103 Valentina Pasquali, "Growing Threat," *Global Finance* 27, no. 5 (May 2013): 21; Ranjan Pal and Leana Golubchik, "Analyzing Self-Defense Investments in Internet Security under Cyber-Insurance Coverage" in 2010 IEEE International Conference on Distributed Computing Systems, 1–9, doi:10.1109/ICDCS.2010.79.

104 Mason Rice, Robert Miller, and Sujeet Shenoi, "May the U.S. Government Monitor Private Critical Infrastructure Assets to Combat Foreign Cyberspace Threats?" *International Journal of Critical Infrastructure Protection* 4, no. 1 (April 2011): 3–13, doi:10.1016/j.ijcip.2011.02.001.

105 Pasquali, "Growing Threat."

106 Butler W. Lampson, "Computer Security in the Real World," *Computer* 37, no. 6 (June 2004): 37–46.

enhance our security posture.[107] Pal and Golubchik argue that, if the cost of defensive security measures were defrayed through a partial "insurance" fee, the adoption rate by private industry owners would be much greater.[108] Although this avenue is interesting, other experts disagree, stating that voluntary measures will never provide for a more robust defensive cyber-security stance.[109]

One of the aspects of defensive cyber security proposed by DHS has been leveraging the support of the Department of Defense (DOD) and the National Security Agency (NSA). This method would appear to support the department's defensive approach through access to the latest exploits utilized by the nation's premier offensive cyber actors.[110] In this theory, the nation's leading cyber-attack force would provide cyber tools and ways to protect against them so DHS could ensure the defensive tools protecting our nation's infrastructure are infallible. Ross Anderson, in his *Security Engineering* document, disputes the validity of this premise, stating that the intelligence and military community has no reason to provide information that could, if publically exposed, hamper its primary attack mission.[111] Moore, Friedman, and Procaccia, in their paper titled "Would a Cyber Warrior Protect Us?" mathematically demonstrate, through Nash Equilibrium Theory, that this collaborative effort with system defenders is a non-logical choice for the offensive cyber entities of the DOD and intelligence community. The DOD fears that a "zero day" exploit would be publically released and become worthless to them would ensure that they would resist sharing those exploits as to not be in their best interest.[112]

As described by Nigel Martin and John Rice in an article in "Computers and Security," perhaps the point of defensive technology is not necessarily to provide

---

107 Pal and Golubchik, "Analyzing Self-Defense Investments."

108 Ibid., 2.

109 Sofaer and Goodman, "Cyber Crime and Security," 25; Rice, Miller, and Shenoi, "May the U.S. Government Monitor," 2.

110 O. Sami Saydjari, "Defending CyberSpace," *Computer* 35, no. 12 (December 2002): 125–27.

111 Anderson, *Security Engineerin*g, 5.

112 Tyler Moore, Allan Friedman, and Ariel D. Procaccia, "Would a 'Cyber Warrior' Protect Us: Exploring Trade-Offs between Attack and Defense of Information Systems," in *Proceedings of the 2010 Workshop on New Security Paradigms* (New York: 2010 ACM, 2010), 85–94, doi:978-1-4503-0415-3.

security; instead, it is to increase the public's trust in the systems and encourage the use of self-defensive security measures.[113] They argue that most citizens are worried about cybercrime because more than 80 percent of attacks are financially motivated. They further argue that widespread adoption of defensive technology by private citizens would provide the government with increased awareness of the cyber-threat landscape and increased security to the networked world.[114]

The existing literature indicates that the sole utilization of defensive technology provides a measure of security that is far from comprehensive. A purely defensive posture allows attackers unlimited time to identify vulnerabilities in a protected system and to attack that system when it is most advantageous to the attacker. To apply this defensive posture in a physical security setting, a countering force is required to deter an attack from being launched or to cause the attacker to break off the attack.

C. OFFENSIVE (DETERRENT) OPERATIONS IN CYBER SECURITY

In her article "At light speed: Attribution and Response to Cybercrime, Terrorism and Warfare," Susan Brenner establishes that societies have always sought to maintain order to survive and prosper. Brenner maintains that, in the modern era, internal threats to order were dealt with through law enforcement, while external threats were dealt with through military action.[115] For the purpose of this thesis, the description of cyber-attack deterrence obtained through offensive action refers primarily to actions conducted by law enforcement officers but does not discount the need for actions undertaken by the military or intelligence community. Any offensive action is guided by existing statute or U.S. government guidance and is conducted to eliminate an existing threat and result in increased cyber security through deterrence. This assumption is supported in M.E. O'Connell's article, "Cyber Security without Cyber War," on maritime piracy—which has been successfully countered by military units operating in a law enforcement

113 Nigel Martin and John Rice, "Cybercrime: Understanding and Addressing the Concerns of Stakeholders," *Computers & Security* 30, no. 8 (November 2011): 803–14, doi:10.1016/j.cose.2011.07.003.

114 Ibid.

115 Susan W. Brenner, "'At Light Speed': Attribution and Response to Cybercrime/Terrorism/ Warfare," *Journal of Criminal Law and Criminology (1973-)* 97, no. 2 (January 1, 2007): 379–475, doi:10.2307/40042831.

action.[116] Supporting this mixing of operational mission is the approach supported by Elizabeth Myers, in her thesis titled "Cyber as a Team Sport: Operationalizing the Whole of Government Approach."[117]

The question of which offensive activity should be undertaken when responding to cyber threats requires careful consideration, as the emerging risks to the nation's infrastructure are dynamic and maturing, and an overly broad application of regulation could negatively impact Internet commerce, innovation, and privacy. Since the initial government directives regarding securing Cyberspace, the DOD, represented by the National Security Agency (NSA) and the newly formed U.S. Cyber Command (CyberCom), moved aggressively to designate cyberspace as a new frontier for warfare with those agencies as the nation's primary offensive actors.[118] DOD's aggressive positioning and publicizing cyberwar as an inevitable, or ongoing, event has highlighted the defense department's belief that military action is the most effective tool available to recognize success in the government's cyber-security mission. Significantly, the DOD belief runs directly opposite to DHS's position that it is the lead agency responsible for the security, defense and resilience of the nation's critical cyber-supported infrastructures.[119]

As recorded by Anderson, a frequently promoted DOD warning is that a well-coordinated cyber attack would ruin the nation's critical infrastructure and result in irreparable damage.[120] But Erik Gartzke, in his "Myth of Cyber War" article, disagrees with this premise, stating instead that a "Cyber Pearl Harbor" is unrealistic.[121]

---

116 M. E. O'Connell, "Cyber Security without Cyber War," *Journal of Conflict and Security Law* 17, no. 2 (August 8, 2012): 4, doi:10.1093/jcsl/krs017.

117 Elizabeth A. Myers, "Cyber as a 'Team Sport': Operationalizing a Whole-of-Government Approach to Cyberspace Operations" (master's thesis, National Defense University, 2011), http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA545638.

118 Levon Anderson, "Countering State-Sponsored Cyber Attacks: Who Should Lead?" in *Information as Power: An Anthology of Selected United States Army War College Student Papers Volume 2*, eds. Jeffrey L. Groh et al. (Carlisle Barracks, PA: U.S. Army War College, 2007), 105–22.

119 "Preventing and Defending Against Cyber Attacks."

120 Anderson, "Countering State-Sponsored Cyber Attacks," 1.

121 Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (October 2013): 2, doi:10.1162/ISEC_a_00136.

Additionally, in his report to Congress, Clay Wilson dismisses this concern because nationally significant cyber-supported infrastructure has become too dispersed and is supported by redundant systems.[122] The review identified that many experts disagree as to whether any entity, including a nation-state level attacker, possesses the capabilities to launch an attack that could overcome the safeguard provided by the redundancy.[123]

Anderson, continuing on the theory that DOD should be the primary entity in securing cyberspace, identifies information systems and cyberspace itself as weapons in the quest for global cyber control.[124] Progressing along this line of reasoning, researcher Matthew Rivera states that cyberspace should be approached in the same way as the Cold War super powers, which featured the premise of deterrence through "mutually assured destruction."[125] William J. Lynn III, flatly dismisses this premise when he states, "Cold War strategies do not apply in cyberspace."[126] The idea of establishing a military "counterstrike" capability was also promoted by Brenner in her review of international laws that may permit attack activity in response to a cyber attack.[127] In contrast, Moore et al. dispute this line of reasoning in regards to "deterrence through strength" and decided that offensively driven cyber units would always err on protecting their own assets and tools and would not publicize their capabilities to aid in deterrence.[128] Additionally, O. Sami Saydjari argues that the militarization of cyberspace should be resisted because the effect of cyber weapons, whose effects can be non-linear, is difficult to predict and could have far reaching consequences.[129]

---

122 Clay Wilson, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress* (Washington, DC: Congressional Research Service, January 29, 2008), 27, http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA477642.

123 Ibid., 24.

124 Anderson, "Countering State-Sponsored Cyber Attacks," 2.

125 Matthew Rivera, "Deterrence in Cyberspace" (master's thesis, Joint Forces Staff College, June 13, 2012), www.dtic.mil/dtic/tr/fulltext/u2/a562428.pdf.

126 William J Lynn, III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, September/October 2010, http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

127 Susan W. Brenner, "Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement?" *Bepress Legal Series,* August 6, 2003, http://law.bepress.com/expresso/eps/15/.

128 Moore, Friedman, and Procaccia, "Would a 'Cyber Warrior' Protect Us?"

129 Saydjari, "Cyber Defense," 4.

Additional arguments against the militarization of cyberspace have been promoted by Gartzke, who disputes whether any act conducted in cyberspace constitutes an 'attack" as defined by international law.[130] Indeed, numerous works produced by military scholars have failed to identify any act conducted in cyberspace that can be identified as constituting an "act of war."[131] In fact, the RAND Corporation produced a work that unsuccessfully sought to identify what constituted an "act of war" and what the appropriate response should be.[132] Some respected governmental leaders, including former DHS Assistant Secretary for Policy Stewart Baker, instead chose a different path and flatly dismissed the need for applicable international laws.[133] The present research also identified a report produced by Martin Libicki, which dismisses the usefulness off a cyber attack in a strategic war.[134]

Interestingly, the Center for Strategic and International Studies' (CSIS) James Lewis also discounted the belief that militarizing cyberspace is required. Lewis, in his publication, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," indicates that cyberwar is not feasible and that most threats from cyberspace involve cyber terrorism, espionage and crime.[135] This premise is directly supported by O'Connell, who instead proposes that the Internet should be viewed as a "sphere of economic and communication activity," the security of which, by law, is the responsibility of domestic law enforcement.[136] Additionally, Gartzke argues that an international requirement of the definition of war is that an element of coercion to force compliance by a government must exist and that, because coercion does not exist during

130 Gartzke, "The Myth of Cyberwar," 8.

131 David M. Keely, Cyber Attack! Crime or Act of War?" (master's thesis, U.S. Army War College, 2011), http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA553344; Rivera, "Deterrence in Cyberspace."

132 Martin C Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=304894.

133 O'Connell, "Cyber Security without Cyber War," 3.

134 Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain," *A Journal of Law and Policy for the Information Society* 8, no. 2 (2012): 326.

135 James Andrew Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats* (Washington, DC: Center for Strategic and International Studies, December 2002), http://www.steptoe.com/publications/231a.pdf.

136 O'Connell, "Cyber Security without Cyber War," 2.

the commission of an anonymous cyber attack, the activity cannot be viewed as an act of war.[137]

In contrast to the effort to militarize cyberspace, the activities identified by Lewis and the environment described by O'Connell are internationally recognized as the domain of law enforcement. The view that cybercrime, cyber terror and cyber espionage are best dealt with through law enforcement means is supported by scholarly works.[138] To further muddy the waters, according to McHugh et al., an attacker typically has been characterized by the motivation for his or her attack or the risk the attacker poses to the victim. This methodology has been difficult to apply to threats emanating from the cyber world,[139] but it is more easily defined in the examination of criminal statistics, where impact can be directly measured. The requirement to identify an attacker's motivation to help decide on a proper national response is of such importance that Kristin M. Finklea and Catherine A. Theohary specifically mention its importance to Congress in a Congressional Research Report.[140]

These tensions speak to one of the most important issues regarding cyber-based threats to U.S. infrastructure: successfully attributing the malicious action to a specific actor in an attempt to identify the actor's motivation for the attack. Wilson described the difficulty in attribution as the major issue in identifying the intent behind the attack.[141] Further, he identified that malicious actor's use of highly advanced cyber-attack tools and techniques and their tendency to operate from "safe havens" with the possibility of nation-state support further complicating attribution.[142] Brenner also described attribution of the cyber attacker as one of the major hurdles in the successful law

---

137 Gartzke, "The Myth of Cyberwar," 14.

138 Kristin M. Finklea and Catherine A. Theohary, *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement* (CRS Report No. R42547) (Washington, DC: Congressional Research Service, July 20, 2012), 2, http://digital.library.unt.edu/ark:/67531/metadc98020/ metadata/?q=cybersecurity%20cybercrime.

139 McHugh, Christie, and Allen, "Defending Yourself."

140 Finklea and Theohary, *Cybercrime Conceptual Issues*, 2.

141 Wilson, *Botnets, Cybercrime, and Cyberterrorism, 33*.

142 Ibid., 13.

enforcement pursuit of cyber actors,[143] and the difficulty in attribution is of such significance that it has also been highlighted in numerous reports to Congress.[144]

In earlier works, Brenner promoted the idea that law enforcement provides society a baseline level of security and that the main mission of law enforcement is to discourage bad behaviors deemed unacceptable by society.[145] Brenner also argued that law enforcement was successful against traditional crime because criminals were constrained by physical proximity (criminal to victim), scale (person to person) and pattern. Brenner further claimed that the cyber world changed those aspects of crime and that law enforcement has become less effective.[146] Abraham Sofaer and Seymour Goodman disagree with this premise and indicate that law enforcement is still effective against cyber-based threats and does provide a deterrent effect through aggressive law enforcement that has adapted to the changing requirements of cyberspace.[147] Myers also stresses that a strong deterrence policy would clearly indicate to potential attackers the ramifications of their activities.[148]

Flowers et al., within their review of existing laws, specifically addressed the need for the penalty to the attacker to be severe enough to act as deterrent.[149] Flowers shows that the main U.S. law against cyber intrusions, Title 18 United States Code 1030, is a cyber-security law.[150] A review of surveys conducted by two leading cyber-security and defense firms show that the vast majority of malicious cyber activity was classified as financially motivated cybercrimes.[151] These reports indicate that the majority of

143 Brenner, "At Light Speed," 28.

144 Finklea and Theohary, *Cybercrime*.

145 Brenner, "Toward a Criminal Law for Cyberspace," 6.

146 Ibid., 71.

147 Sofaer and Goodman, "Cyber Crime and Security."

148 Myers, "Cyber as a 'Team Sport.'"

149 Angelyn Flowers, Sherali Zeadally, and Acklyn Murray, "Cybersecurity and U.S. Legislative Efforts to Address Cybercrime," *Journal of Homeland Security and Emergency Management* 10, no. 1 (April 13, 2013): 1–27.

150 Ibid., 5.

151 "2013 Trustwave Global Security Report," Trustwave, accessed October 2, 2013, https://www2.trustwave.com/2013GSR.html.

malicious cyber attacks should be dealt with through aggressive law enforcement actions that will result in the elimination of the threat or the deterrence of future activities.[152]

Frederic Lemieux, in his article "Investigating Cyber Security Threats," concurs with Brenner's assumptions that many cybercrimes are traditional crimes committed over the Internet and that the ramifications of the crimes are so far reaching that they require a different approach to deterring them. Lemieux, however, disagrees with Brenner's assumptions of non-adaptation and instead proposes that cyber-law enforcement entities have adapted and become proactive and preventative.[153] Lemieux postulates that cybercrimes are still committed by humans and a human can be deterred from committing criminal acts when attribution can be made.[154] Central to this deterrence is the possibility of apprehension, and the belief that cyber-law enforcement has become less reactive and more in line with the principles of "Intelligence Led Policing" (ILP). ILP is, by definition, a proactive law enforcement activity that specifically targets the highest levels of threats to either eliminate the threat OR harden the target of the attack.[155] The goal of hardening the defenses calls for information derived from cyber investigations to be used to provide greater cyber-security awareness to our nation's critical infrastructure. Even Dr. Brenner agrees that proactive law enforcement is useful as a method of deterrence and provides a measureable method of preventing future attacks.[156]

D. CONCLUSION AND EXISTING GAPS

The existing research into the threats against U.S. critical cyber infrastructure has generally focused on two key areas, namely defensive security utilizing technology and offensive operations that identifies and eliminates the actors who seek to target our cyber

---

152 "2013 Data Breach Investigations Report," Verizon Enterprise Solutions, accessed September 29, 2013, http://www.verizonenterprise.com/DBIR/2013/.

153 Frederic Lemieux, *Investigating Cyber Security Threats: Exploring National Security and Law Enforcement Perspectives* (Washington, DC: Cyber Security Policy and Research Institute: George Washington University, 2011), 1–13, http://www.cspri.seas.gwu.edu/Seminar.pdf.

154 Ibid., 8.

155 Ibid., 3.

156 Brenner, "Toward a Criminal Law for Cyberspace, " 78.

systems. Most scholars believe the threats emanating from cyberspace will continue to grow in frequency and sophistication. Additionally, a reliance on technology-driven security methods, while marginally effective, is insufficient to ensure cyber security. Additional research is needed to evaluate the effectiveness of the defensive and offensive approaches, and if a deterrent effect can be quantified and proven to affect cyber threats.

IV. ANALYSIS OF EVOLVING CYBER SECURITY MISSIONS AND FOCUS

Chapter III provided an overview of the available governmental, academic, and private sector literature in the rapidly expanding field of cyber security best practices and technology. Additionally, the applicable government laws and policies, as well as the primary agencies, responsible for the security of the nation's cyber supported critical infrastructure were reviewed and analyzed to frame the discourse between the leading experts regarding whether the deployment of defensive technology or offensive operations resulting in a deterrent effect is considered most effective in defending against cyber intrusions.

Chapter IV provides an overview of the evolution of the DHS cyber security mission, the department's gravitation to technology supported cyber defense and information sharing initiatives and the hesitation to utilize DHS law enforcement agencies and their lawful authorities. Additionally, the evolving cyber security missions of the NSA (inclusive of DOD/Cyber Command), the FBI, and the USSS are described as these four entities have the broadest authorities in the cyber security and enforcement arena.

A. DEPARTMENT OF HOMELAND SECURITY

With the passage of the The Homeland Security Act of 2002 (HSA), which formed the Department of Homeland Security (DHS) and provided the department with its legal authorities and mission, the greater U.S. government turned its attention to enhancing and developing other departments.[157] Although the primary mission of the department was to prevent terrorist attacks; lessen the nation's vulnerability to terrorist attack; minimize damage from attacks; and increase the national resiliency, initially cyber security was a secondary concern and responsibility of DHS.[158] Recognizing that many existing government agencies possessed homeland security related capabilities and

[157] Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002).

[158] Ibid.

authorities; HSA identified agencies that were organizationally re-aligned under the new department while also forming new component agencies through the combining of multiple existing agencies or missions.[159]

Although the impetus for the formation of DHS was specifically in response to the terrorist threat, the inclusion of the Federal Emergency Management Agency (FEMA), which was the primary government authority in responding to mass casualty or resiliency events, unknowingly provided the department a wider prism through which to pursue the homeland security mission.[160] This expanded mission space offered the new department avenues of growth that quickly enabled it to grow its influence beyond terrorist attack prevention, response, and mitigation, and move aggressively into an "all hazards" approach to homeland security.[161] Unfortunately, according Dara Cohen, Mariano-Florentino Cuellar, and Barry Weingast, this "all hazards" approach resulted in some DHS agencies being forced to de-emphasize their legacy missions to fulfill the new requirements of the department.[162]

Among the 22 agencies realigned under the newly formed department were the U.S. Secret Service (USSS) and the U.S. Coast Guard (USCG), two agencies that struggled to retain their identities and unique history while still adding value to the new department. For the U.S. Secret Service, an agency that had been a valued member of the U.S. Treasury Department since the agency was formed in 1865, realignment to a department that had limited interest in financial crime investigations and executive/dignitary protection was tumultuous. Unrecognized by many within the agency during those early years in DHS, portions of the department's rapidly evolving mission positioned the USSS, its cyber capabilities and financial crimes investigative authorities at the forefront of the growing departmental mission of cyber security operations.

Although DHS's initial focus on terrorism related matters and its increasing gravitation towards an "all hazards" approach to homeland security could appear to be an

159 Ibid.

160 Cohen, Cuéllar, and Weingast, "Crisis Bureaucracy."

161 Ibid., 26.

162 Ibid., 27.

instance of "mission creep"; this research identified that the U.S. government had been steadily moving towards an "all hazards" approach since the 1990s. Since that time, the government had been gaining better understanding of the interconnectivity and vulnerability of the nation's identified CIKR to terrorist attack or other disruption through cyberspace. As identified by Fleming and Goldstein of the Homeland Security Studies and Analysis Institute, the government shift reflected the realization that cyberspace forms the unpinning of the bulk of the nation's CIKR including banking and finance, communications and transportation.[163] The quickly evolving importance of cyberspace in our nation's functioning, combined with the department's CIKR-centric mission developed by previously identified legislation and presidential directives caused the rapid development of the cyber security focus of the department. Fleming and Goldstein also documented DHS's determination that comprehensive cyber security measures could be described in three main categories: 1) System and Information Protection, 2) Information Sharing and 3) Incident Response.[164] The development of the department's cyber security efforts slowly, but demonstratively, tracked towards building new operational entities and away from leveraging the department's legacy agencies such as the Secret Service.

In an early indicator of problems the department and its component agencies would face in the future, efficiency reviews conducted in 2005 by the Government Accountability Office (GAO) indicated that, although the HSA had designated DHS to lead the government's critical infrastructure and cyber security efforts, the department lacked the legal authorities necessary to achieve success.[165]

As referenced earlier in this thesis, President Bush's 2008 Comprehensive National Cyber-Security Initiative (CNCI) was one of the first governmental documents issued after DHS's creation that specifically addressed the importance of the cyber world

163 Fleming and Goldstein, *An Analysis of the Primary Authorities*.

164 Ibid., 26.

165 U.S. Government Accountability Office (GAO), *Critical Infrastructure: Challenges Remain in Protecting Key Sectors* (Washington, DC: GAO, July 19, 2005), 2.

in our nation's security.[166] This document set the course for the government's cyber security progress through identifying the areas of concentration of efforts. In light of the three categories defined above, DHS's gravitation towards technology solutions and building mission specific internal components seems a natural progression. Additionally, the CNCI directed departmental efforts toward developing government wide programs regarding "trusted connection" programs; Intrusion Detection and Prevention Systems (IDS/IPS); Research and Development (R&D) of new technology; information sharing initiatives and other technology centric solutions.[167] Although the need for law enforcement operations and budgetary increases for law enforcement were offered in the CNCI, only one of the 12 initiatives outlined within the document referenced any measure of deterring cyber attackers from intruding into protected systems.[168]

In February 2010, with the release of the *Quadrennial Homeland Security Review* (*QHSR*), DHS defined the course of the department and the core mission areas that would receive the most scrutiny and support. This seminal document identified weapons of mass destruction and terrorist attacks against the homeland as the top priorities for the department but identified cyber threats and protecting civil liberties and privacy as the third focus area for department resources.[169] To account for the cyber threat, the *QHSR* identified the areas of developing system monitoring tools, managing cyber risk, developing cyber skills and information sharing as well as developing a cyber incidence response plan to be of primary importance for the department.[170] The department's development of the U.S. Computer Emergency Response Team (U.S.-CERT) and other internal cyber response teams, as opposed to utilizing component agencies that already operated within the cyber security mission, was recognized within the Secret Service as a de-valuing of the agency and its mission. That same year, DHS's Inspector General reviewed the U.S.-CERT program and noted that, although progress had been made

166 "The Comprehensive National Cybersecurity Initiative."

167 Ibid.

168 Ibid.

169 U.S. Department of Homeland Security (DHS), *Quadrennial Homeland Security Review* (Washington, DC: DHS, February 2010), https://www.hsdl.org/?view&did=29742.

170 Ibid., 29.

regarding information sharing, U.S.-CERT lacked the statutory enforcement and response authority required for success.[171]

Continuing the progression, the 2010 release of the *Bottom Up Review* (*BUR*), further identified the department operations and future areas of concentration and expansion. Although the *BUR* recognized the diverse mission space of the department including immigration, border and cyber security, financial crimes investigations, and terrorism, the *BUR* specifically referred to being authorized by statute to secure civilian networks, and to defend government and civilian networks.[172] The *BUR* also designated the newly formed DHS-National Protection and Program Directorate (NPPD), which had resulted from an earlier re-organization of the National Preparedness and Protection Directorate, as the primary coordinating entity to secure and defend the CIKR from cyber attack.[173] The *BUR* went on to highlight the efforts of the National Cyber and Communications Integration Center (NCCIC) and National Cyber Security Division (NCSD), as well as the importance of the deployment of defensive and identity management technology as central to the department's efforts.[174]

The department's focus on defensive technology, development of response capabilities activities, and the apparent dismissal of the deterrent effect of component law enforcement action, was specifically acute for the USSS as the agency struggled to blend with the department. The department's reliance on executive orders and presidential directives, which highlighted NPPD's lack of the binding legal authority, was especially troubling because the USSS was statutorily authorized as one of the two law enforcement agencies with cyber intrusion investigation authority.[175] Finally, the *BUR* specifically identified that cyber law enforcement coordination and information sharing should occur through the National Cyber Investigative Joint Task Force (NCIJTF) operated by the FBI,

---

171 U.S. Department of Homeland Security (DHS) and Office of Inspector General (OIG), *U.S. Computer Emergency Readiness Team Makes Progress in Securing Cyberspace, but Challenges Remain* (Washington, DC: DHS and OIG, June 2010), 9.

172 DHS, *Bottom-Up Review.*

173 Ibid., 21.

174 Ibid., 37–38.

175 Ibid., 40.

as opposed to through it law enforcement agencies or even the department's own NCCIC.[176]

At that time, DHS component agencies were not the only group questioning whether DHS possessed the legal authority to conduct its proposed mission. Fleming and Goldstein, during a 2011 analysis of DHS authorities, identify that although many documents describe DHS as "having the lead" in cyber security, the department did not have the statutory authority to compel other government agencies to comply with departmental demands.[177] That same year, the bi-partisan bill Promoting and Enhancing Cyber Security and Information Sharing Effectiveness Act of 2011 (HR3674) acknowledged that the department lack the statutory authority to conduct or succeed in its cyber security mission and attempted to provide those authorities.[178] Later that same year, the bill failed to be moved from the committee and was removed from consideration.[179]

Later that same year, the department launched a website titled "Preventing and Defending against Cyber Attacks" to publicize the department's cyber security efforts.[180] In another affront to component agencies, the page explained the technology and information sharing programs being conducted by NPPD and failed to reference any DHS law enforcement or component efforts.

The 2011 release of the *Blueprint for a Secure Cyber Future* continued the governmental mandate that cyber security must protect civil liberties and privacy while strengthening the critical infrastructure. Although this publication continued the call for increased use of defensive technology, the department again dismissed its cyber law

176 Ibid., 41.

177 Fleming and Goldstein, *An Analysis of the Primary Authorities,* 9.

178 Brian Hammond, "Cybersecurity Bill Would Clarify DHS Role, Create Info-Sharing Body," *Cybersecurity Policy Report,* December 19, 2011.

179 "H.R. 3674 (112th): PRECISE Act of 2012," *GovTrack.us,* accessed May 11, 2014, https://www.govtrack.us/congress/bills/112/hr3674.

180 "Preventing and Defending Against Cyber Attacks."

enforcement agencies by designating the NCCIC and NCIJTF as the primary cyber incident response entities.[181]

In September 2011, DHS-OIG released another report that reviewed the department's information sharing and cyber security activities. Although gains had been made within certain fields, the review identified that U.S.-CERT and NCCIC had poorly defined and misunderstood mission capabilities.[182] The report also continued to identify that the department lacked the statutory authority to respond to and mitigate cyber threats, without consideration for the department's component agencies.[183]

In 2012, in another direct confirmation that the department lacked the authorities to conduct its cyber security mission, Senator Joseph Lieberman introduced Senate bill S 2105, the Cyber Security Act of 2012.[184] This bill, like many others before and since, failed to move from committee and was removed from consideration.[185]

Most recently, in 2013, GAO released another audit of the department's effectiveness in the cyber security mission. GAO again called for Congress to pass legislation granting the department statutory authorities to compel system owners' compliance to mandates and cyber security initiatives.[186] This GAO report also identified that the department lacked the authority to force other government agency's cyber security compliance.[187] Missing from any of these efforts or reports was recognition that portions of DHS, namely the USSS, was supported by the Federal Criminal Code in its

---

181 DHS, *Blueprint for a Secure Cyber Future*.

182 Charles Edwards, *Review of the Department of Homeland Security's Capability to Share Cyber Threat Information* (OIG Report 11-117) (Washington, DC: Office of the Inspector General, September 2011).

183 Ibid., 29.

184 "Text of S. 2105 (112th): Cybersecurity Act of 2012 (Placed on Calendar in the Senate Version)," *GovTrack.us*, accessed October 14, 2013, http://www.govtrack.us/congress/bills/112/s2105/text.

185 "Cybersecurity Act of 2012 (2012S. 2105)," *GovTrack.us*, accessed May 11, 2014, https://www.govtrack.us/congress/bills/112/s2105.

186 Gregory C. Wilshusen and Nabajyoti Barkakati, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented* (GAO-13-187) (Washington, DC: Government Accountability Office, February 2013), http://www.gao.gov/products/GAO-13-187.

187 Ibid.,52.

enforcement action and, through the issuance of subpoenas and search warrants, could force compliance of system owners.

A review of the department's cyber security budget requests provides another poignant indicator of the support DHS provided to NPPD to develop defensive cyber technology in relation to the allocation provided by the department to component agencies with statutory cyber security authorities, namely the USSS. According to the 2009 DHS "Budget in Brief," the NPPD budget request allocated $1.28B in funding and 849 Full time equivalent (FTE) staffing positions compared to the USSS request for $1.63B and 6732 FTE.[188] By the 2011 budget request, NPPD's request had climbed to $2.36B with 2969 FTEs whereas the USSS request remained relatively flat at $1.81B and 7,014 FTEs.[189] More recently, in 2013, during the ongoing government budget crisis and sequestration, the NPPD request settled at $2.51B with 2,787 FTEs compared to the USSS request for $1.85B distributed to 7,061 FTEs.[190]

B. NATIONAL SECURITY AGENCY AND DEPARTMENT OF DEFENSE

As a means of ensuring their security, nations have always sought information and the ability to monitor the communications of other nations and their enemies. Throughout the early 20th century, small military units were developed to concentrate on the interception and exploitation of foreign communications, a process that became known as communications intelligence (COMINT).[191] This section reviews the development of the NSA, the adaptation of the agency to the developing communication methods of the Digital Age, and the expansion of the agency's original mission and operational restrictions. From its unremarkable beginnings, the NSA has developed the field of COMINT, currently identified as signals intelligence (SIGINT), to become one of

188 "2009 DHS Budget in Brief," U.S. Department of Homeland Security, February 4, 2009, http://www.dhs.gov/xlibrary/assets/budget_bib-fy2009.pdf.

189 "2011 DHS Budget in Brief," U.S. Department of Homeland Security, February 2011, http://www.dhs.gov/xlibrary/assets/budget_bib_fy2011.pdf.

190 "2013 DHS Budget in Brief," U.S. Department of Homeland Security, accessed September 26, 2014, http://www.dhs.gov/xlibrary/assets/mgmt/dhs-budget-in-brief-fy2013.pdf.

191 *Wikipedia*, s.v. "National Security Agency," accessed May 13, 2014, http://en.wikipedia.org/w/index.php?title=National_Security_Agency&oldid=608427380.

the most technologically advanced and effective intelligence collection agencies in the world which has also positioned itself at the forefront of the government's efforts at countering the threat resulting from the spread of international terrorism and the developing cyber world.

Following the passage of the National Security Act of 1947, in 1952 President Truman issued National Security Council Intelligence Directive No. 9 (NSCID-9), which authorized the Department of Defense (DOD), under the direction of the Secretary of Defense, to conduct the mission of the interception, collection and analysis of the communications of foreign governments and individuals to support military operations.[192] To accomplish this, NSCID-9 directed the formation of the National Security Agency (NSA), which was formed "to provide an effective, unified organization and control of the communications intelligence activities of the United States conducted against *foreign governments* [Italics added]"[193] NSCID-9 also mandated that a NSA Director, who was required to be a U.S. military commissioned officer of at least a 3-star rank, would manage and direct the COMINT operations of the NSA. This directive did not reference the need to protect our citizens' constitutional rights against unreasonable search and seizure or our right to privacy but it did stress that COMINT was to be directed against foreign threats.

With the rapidly increasing use of technology and mass communication devices, the NSA experienced exponential growth in both the scope of its mission and its capabilities. In 1971, Secretary of Defense (SECDEF) Lovett issued Department of Defense (DOD) directive S-100.20, to further define the authorities, functions and mission of the NSA, which was specifically identified as a separate agency within the DOD operating under the direction of the SECDEF.[194] Due to the increase in collection platforms and technology exploited by the NSA, this directive renamed the overarching target of the NSA as SIGINT, which included COMINT (communications intelligence),

---

192 Harry Truman Administration, *National Security Council Intelligence Directive No. 9* (Washington, DC: White House, December 29, 1952).

193 Ibid.

194 Department of Defense, *Department of Defense Directive S-5100.20* (Washington, DC: Secretary of Defense, December 23, 1971).

ELINT (electronic intelligence) and Telemetry Intelligence (TELINT). This rebranding of the targets of the agency indicates that the agency had expanded its methods of collection from solely communication intercepts to all methods of electronic exploitation.[195] Finally, this directive, although specifically addressing that the NSA should not engage in censorship or monitoring of the press, made no reference to protecting the citizens' rights were addressed.[196]

The 1960s and early 1970s were a turbulent time in the U.S. as the nation struggled with the de-escalation of the Vietnam War, political unrest, the equal rights movement, and the revelation that the U.S. intelligence community (IC) had violated or circumvented laws at the direction of various presidential administrations to domestically collect information and target U.S. citizens for their constitutionally protected activities.[197]

In 1976, the U.S. Senate Select Committee to Study Governmental Operations, led by Senator Frank Church, held hearings and produced a report (hereinafter "the Report") to document the government's abuses of its citizens' rights and to offer guidance on intelligence activities.[198] The Church Report acknowledged that few laws or regulations regarding the collection of intelligence targeting Americans existed and that the IC must be subject to the rule of law because it had grown so vast that it required governmental oversight.'[199][200] This finding was supported by a 1972 U.S. Supreme Court ruling, known as the *Keith* ruling, that although domestic intelligence collection must operate through the traditional legal process, Congress could establish a special court to review foreign intelligence surveillance operations.[201] The Report also sought to ensure

195 Ibid.

196 Ibid.

197 "Final Report S. Rep No.94-755," U.S. Select Committee to Study Governmental Operations On Intelligence, accessed September 26, 2014, http://www.intelligence.senate.gov/churchcommittee.html.

198 Ibid.

199 Ibid.

200 Ibid.

201 Andrew Nolan and Richard M. Thompson, III, *Reform of the Foreign Intelligence Surveillance Courts: Procedural and Operational Changes* (CRS Report R43362) (Washington, DC: Congressional Research Service, 2014), 5.

that future administrations did not utilize the IC for political gains and mandated that no future executive actions or directives could counteract the commission's findings.[202]

Due to documented violations of law by the Central Intelligence Agency (CIA), NSA, and FBI, the Report authorized the FBI solely, under strict guidance and oversight, to conduct domestic intelligence activities.[203] The NSA was forbidden to monitor any domestic communications, even for foreign intelligence purposes and the agency was not permitted to collect any citizen's communication unless the collection was conducted in accordance with Title III of the Omnibus Crime Control Act with proper judicial review.[204] Also contained within the report was the requirement that the NSA should never be permitted to request a commercial carrier to capture and provide communications that the NSA could not legally obtain under the Church Report requirements.[205] Arguably, the findings of the Church Commission exposed the NSA to greatly increased oversight and forced the agency to adjust their collection activities into compliance. However, in line with developing, innovative technology, the agency continued to position itself aggressively to exploit new venues of collection from communication platforms that had yet to be developed.

In 1978, drawing on the *Keith* Ruling and Church Committee hearings, the Congress initiated the Foreign Intelligence Surveillance Court (FISA) to provide judicial oversight to the IC.[206] The FISA court judges were required, through a non-public court proceeding, to review an agency's request to conduct domestic intelligence and signals intelligence operations. It was envisioned that, through the FISA court, the privacy and civil liberties of our citizens would be ensured while maintaining the focus of the IC towards foreign governments and adversaries.[207] Within this framework, during the draw down from the Cold War, increasingly disbursed regionalized threats, terrorism, the

202 "Final Report S. Rep No.94-755."

203 Ibid.

204 Ibid.

205 Ibid.

206 Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, Stat. 1783 (1978).

207 Nolan, Thompson, and Richard, *Reform of the Foreign Intelligence Surveillance Courts,* 6.

rapidly evolving cyber world, and online communication platforms, NSA continued to evolve and invest in the capability to provide more comprehensive SIGINT support to the U.S. government.

In 1981, President Reagan issued Executive Order (EO) 12333, which sought to describe and guide U.S. intelligence activities and agencies to ensure effective, efficient, and lawful operations. One of the primary goals described in EO 12333 was to ensure that our citizens' rights and privacies were protected during intelligence collection activities.[208] Of particular note is that the Director of the FBI was specifically the only entity approved to coordinate all domestic clandestine foreign counter-intelligence collection through both human and human-enabled sources.[209] The Director of the CIA meanwhile, was authorized to coordinate all foreign intelligence collection of human and human-enabled sources.[210] NSA was solely authorized to collect, analyze and report signals intelligence in support of the DOD counter intelligence mission and to operate a domestic administrative operations to provide cover support to the other intelligence agency's operations.[211]

In 1993, then NSA Director J.M. McConnell issued U.S. Signals Intelligence Directive (USSID) 18, which described the legal compliance and minimization process for NSA SIGINT operations.[212] The primary driver behind this document was to ensure that the SIGINT operations were conducted to safeguard the constitutional rights of U.S. persons.[213] The document quotes the Fourth Amendment of the Constitution and refers to the U.S. Supreme Court ruling that warrantless interception of communications constitutes an illegal search and seizure in violation of the Fourth Amendment.[214] Later in the directive, McConnell states that it is the policy of NSA to target and collect only

---

208 Exec. Order 12333 C.F.R. 200 (1981).

209 Ibid.

210 Ibid.

211 Ibid.

212 National Security Agency (NSA), *United States Signals Intelligence Directive (USSID) 18–Legal Compliance and Minimization Procedures* (Washington, DC: NSA, July 27, 1993.

213 Ibid.

214 Ibid.

significant foreign intelligence communications.[215] In another section, the directive denies collection authority in a situation where a person is not acting on behalf or at the direction of a foreign power, but whose actions could benefit a foreign power.[216]

These previously described documents clearly indicate that, barring early missteps by the IC, the NSA was cognizant of the importance of the rights that form the underpinnings of this nation. Although volumes of classified documents and directives exist which will be outside the scope of this thesis, it is well documented that the NSA was conceived as a civilian intelligence collection agency, organizationally aligned, managed and supporting the DOD, with a mandate to target and collect foreign government and military communications. The 1990s Internet boom, proliferation and mass adoption of email and other Internet supported communication systems, and the increasingly borderless nature of cyber space changed the way the world interacted. Physical proximity, access, and national borders were suddenly less important to our daily interactions as commerce, communication, and crime, including espionage, were increasingly conducted through cyberspace. As communications and cyber space continued to evolve, the NSA was positioned to be more central to the mission of securing the country; a position that promised funding, staffing and authorization increases. But technology was not the only rapid development of the 1990s; through a series of terrorist attacks targeting our facilities, personnel and interests overseas, the nation became aware that not all physical threats emanated from hostile nations.

On September 11, 2001, the threat from terrorism was brought into the home of every American, causing widespread panic and demands to ensure our citizens' security. In the days immediately following the attacks of 9/11, the Bush administration established a framework to guide and codify the changes that he had indicated were neccesary in his public address following the attacks. These early decisions and efforts resulted in sweeping organizational and targeting changes for the U.S. intelligence program; and a marked change in public acceptance of the level of government impact

215 Ibid.

216 Ibid.

into citizens' privacy in an focused effort to defeat the perceived threat from international terrorism.

On October 21, 2001, the passage of the USA Patriot Act (public law 107–56) codified the expansion of the IC's authorities and focused the resources of the federal government to our nation's security on predominantly non-nation state enemies.[217] Among the far-reaching changes to IC authorities and missions contained within the Act was section 214, which amended FISA targeting requirements from being "foreign intelligence and international terrorism information" to "information collected that is *likely* to contain foreign intelligence information or international terrorism information [italics added].[218] It can be argued that this small alteration decreased the NSA's collection restrictions while providing a rapid expansion of opportunities that no longer had to testify that the target was an agent of a foreign intelligence group; in effect, being a criminal that may be connected to foreign intelligence was sufficient. Additionally, section 802 included a new definition of domestic terrorism, which is described as domestic acts that are 1.) Dangerous to human life and /or a *violation of the criminal laws of the U.S. or a state* and; 2.) Are intended to coerce a government or the population [italics added].[219] However, the alterations to section 814 provided NSA with one of its most important tools to expand its area of operation within the developing cyberspace. Section 814, titled "Deterrence and Prevention of Cyber Terrorism" alters Title 18 United States (criminal) Code 1030 – "Fraud and related activity in connection with computers" to make any cyber attack which results in "damage to any computer system used by or for a government entity in furtherance of the administration of justice, national defense, *or national security*" [italics added].[220] The addition of a national defense clause to Title 18 USC 1030 continued to blur the lines of law enforcement and intelligence operations and targets.

---

217 USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

218 Ibid..

219 Ibid.

220 Ibid.

In that short period after 9/11, alterations to existing criminal statues, and to the authorities of law enforcement, the IC, and the NSA/DOD in particular, initiated major changes to many aspects of our citizens' lives and how the government interacted with them. Supporters and detractors all voiced opinions regarding the lawfulness and appropriateness of these changes but, in the aftermath of the worst terrorist attack and loss of life in America, the rush to identify the enemy and provide security to the populace was the government's primary goal.

This changing perspective was exemplified in a 2002 National Defense University article calling for allowing domestic military operations because the "frontline," which had always been located in foreign locales, was now inside the homeland and should be considered as a "domestic battle space."[221] The speed with which military proposed this idea is of note because the post-9/11 period was the military's best opportunity to propose a review of the Posse Comitatus Act, which prohibits the domestic use of the military except in very specific situations, including civil disturbance/insurrection, counterdrug operations, and disaster relief.[222] For the NSA, a DOD aligned civilian intelligence agency, which had just gained additional mission spaces through the Patriot Act, the limits of expansion relied only on itself and how the governmental discourse could be shaped.

In another step that blurred the lines between domestic and foreign operations by the government, on May 17, 2002, the FISA Court issued a judgment in response to a Department of Justice (DOJ) memorandum calling for the discontinuance of the "wall" between law enforcement and intelligence operations.[223] This wall was the prohibition of sharing information received during intelligence and law enforcement operations as a means of ensuring that the collecting authority adhered to civil and privacy protections. Within the IC community, this opened up the possibility of utilizing information derived

---

221 Steven J. Tomisek, *Homeland Security: The New Role for Defense* (Washington, DC: Institute for National Strategic Studies, National Defense University, 2002), 1.

222 Ibid., 6.

223 Elizabeth B. Bazan, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions*, CRS Report RL3046 (Washington, DC: Congressional Research Office, February 15, 2007), 5.

from domestic operations, even though it may contain U.S. person information, to develop a better common operating picture with little oversight.

Also during this time period, as described in other sections of this thesis, increasing numbers of respected sources began to propose and promote the possibility of cyber war and cyber terrorism. The basis for these assumptions was rooted in the fear that nation-states or cyber-terrorists could launch disruptive cyber attacks against the nation's critical infrastructure because of the nation's increasing reliance on the Internet. For example, a December 2002 article in *Computer* magazine written by O. Sami Saydjari proposed that the nation's cyber supported critical infrastructure was highly vulnerable to cyber attack and that the president should initiate a Cyber Warfare Defense Project modeled after the nation's "Manhattan Project."[224] Although the threat of cyber war or cyber terror was dismissed as unrealistic or ineffective by James Lewis of the Center for Strategic and International Studies as the decade progressed, the media increasingly promoted the threat of cyber terrorist attack or nation-state sponsored cyber warfare.[225]

By January 2006, a letter from U.S. Attorney General (AG) Alberto Gonzalez to Senator William Frist, offered proof of how successfully and completely the IC, in this case the NSA, had asserted the legality and appropriateness of allowing the IC to operate domestically to ensure success in the pursuit of homeland security. Gonzalez promoted that the collection of any communications into, or out of, the country, which may be connected to terrorism or *national security* was lawful and consistent with civil liberties [Italics added].[226] Interestingly, in this letter, AG Gonzalez referred to Congress's authorization of the President's deployment of the military (NSA) to conduct warrantless interception of communications as being consistent with presidential powers during war times.[227] Finally, Gonzalez argued that FISA and Title III communication interception requirements did not apply to wartime intelligence collection that must be utilized to

---

224 Saydjari, "Defending Cyber Space."

225 Lewis, "Assessing the Risks of Cyber Terrorism."

226 Alberto Gonzales, "Legal Authorities Supporting the Activities of the National Security Agency Described by the President," January 19, 2006, http://web.elastic.org/~fche/mirrors/www.jya.com/2012/06/doj011906.pdf.

227 Ibid.

ensure enduring homeland security.[228] Although this letter specifically addresses terrorism, the blurring of the lines in an effort to provide homeland security, effectively allowed the NSA to operate without regard to national boundaries. When applied to cyberspace, this approach removed any previous collection-targeting requirement that required specificity instead; the NSA was now free to collect any information flowing through the borderless cyber world.

The evolution of the public discourse regarding cyber war, cyber terrorism, the expansion of the NSA's collection authority, and the removal of collection and operation restrictions, quickly progressed. In June 2009, then SECDEF Robert Gates established the military's U.S. Cyber Command to defend against the perceived increasing threats to the U.S. government, military and commercial information systems from what was reported as our adversary's rapidly developing network attack capabilities.[229] Mark Young, in a Journal of National Security Law and Policy article, proposed that civilian agencies, including DHS and law enforcement, lacked the capacity to defend the country from national security cyber threats and that the military was the only government asset capable of the mission.[230] Although acknowledging that Cyber Command lacked guiding doctrines regarding the use of cyber power and computer network operations, Young proposed that authorizing DOD to lead the nation's cyber security efforts was proper because cyberspace must be treated like the other war fighting domains of sea, air, land, and space.[231] In addition to the previously described expansion of the NSA's intelligence collection authorities, the framing of cyber space as a military sphere of operation also benefitted the agency since it was a civilian intelligence agency aligned within the U.S. military structure.

Further ensuring the NSA's premier positioning within the government's cyber security apparatus, on May 21, 2010, SECDEF Gates appointed the Director of the NSA,

---

228 Ibid.

229 Mark D. Young, "National Cyber Doctrine: The Missing Link in the Application of American Cyber Power," *Journal of National Security Law & Policy* 4, no. 173 (2010): 173.

230 Ibid., 174.

231 Ibid, 175.

Army General Keith Alexander, to assume "dual hatted" command of U.S. Cyber Command.[232] By placing a single commander over both the civilian intelligence agency, with its unique authorities and capabilities, and the military's cyber attack forces, the lines of distinction were removed. Opponents proposed that this allowed for the General to utilize whichever portion of his command as necessary to operate within cyberspace without regard for national boundaries, civil liberties, and the Posse Comitatus Act, while placing too much power within one organization.[233]

Supporting opponents' fears, only two years later, in November 2012, President Obama issued PPD-12 (classified), as reported by the Washington Post. According to the Post, PPD-12 authorized U.S. Cyber Command to enact more aggressive efforts in defense of government *and* private computer networks [italics added].[234] And a few months later, on February 12, 2013, President Obama issued PPD-21, Critical Infrastructure Security and Resilience. Although it does not refer specifically to the NSA, PPD-21 authorizes the IC, under the direction of the Office of the Director of National Intelligence (ODNI), to exercise its authority over national security cyber systems.[235] In light of the previous administration's defining of critical infrastructure, including cyber space and infrastructure supporting cyber systems, as a national security issue, the inference could be argued that this PD authorizes the NSA to operate within private computer networks.

As described, the development of the NSA, an agency that operates as both a civilian intelligence (SIGINT) collection agency and a military organization, has placed the agency at the forefront of the nation's cyber security efforts resulting in exponential growth of its structure and funding. The world's increasing reliance on the Internet and cyber supported infrastructures allowed the NSA to develop its influence within the

---

232 *Wikipedia*, s.v. "Keith B. Alexander," accessed May 9, 2014, http://en.wikipedia.org/w/index.php?title=Keith_B._Alexander&oldid=604968817.

233 Noah Shachtman, "Military's Cyber Commander Swears: 'No Role' in Civilian Networks," *Wired*, September 23, 2010, http://www.brookings.edu/research/opinions/2010/09/23-military-internet-shachtman.

234 Nakashima, "Obama Signs Secret Directive to Help Thwart Cyberattacks."

235 "Presidential Policy Directive 21: Critical Infrastructure Security and Resilience."

government, and within private cyber supported systems. The NSA's development of domestic collection operations, arguably in direct violation of existing laws and guidelines, requires the nation to decide if the domestic utilization of a military or intelligence agency is a violation of long-held American values. Is the collection and access of citizens' personal information from the Internet by an U.S. intelligence agency a further violation of our citizens' right to privacy? Future chapters will discuss these questions in more detail.

C. FEDERAL BUREAU OF INVESTIGATION

Although common in other countries, a national police force has never existed in the U.S. due to our underlying principles of distributed power, state's rights and limiting federal powers. However, as the nations developed, crimes which crossed state borders became commonplace and, to investigate those crimes and apprehend the criminals responsible, numerous federal law enforcement agencies were formed. In keeping with our underlying values, these federal agencies were authorized specific investigative missions and strict limitations on their operations. Law enforcement officers for these agencies came to be known as "special agents," a title which refers to the agent's limited investigative authorities and not their operational capabilities. The Federal Bureau of Investigation (FBI) has developed to become the most recognized law enforcement agency in the U.S. The FBI is unique among U.S. law enforcement due to its dual mission of criminal investigation and national security (intelligence collection), which has allowed the agency the opportunity to redirect its assets and efforts to counter the most pressing enforcement issues of the day. These dual, sometimes-competing missions have, at times, caused the agency difficulties in the proper allocation of resources, agency infighting and overreach of authority.

Although, at that time, mission-specific federal criminal investigative agencies already existed, in 1908, U.S. Attorney General (AG) Charles Bonaparte hired 10 U.S. Secret Service agents to form the nucleus of an investigative agency operating under the direction and authority of the Department of Justice and the Attorney General. This new investigative agency became known as the Federal Bureau of Investigation (FBI) and was

given the authority to investigate crimes involving inter-state criminal violations under the authority of the Attorney General.[236] Although some in the government feared the FBI would become too powerful due to its rapid expansion, in the buildup to World War I, the agency was given the mission of investigating draft resistors and other violators of the Espionage Act of 1917.[237] This early focus on domestic national security investigations, where the FBI sought to document subversive or foreign intelligence actors, including reported communist and Nazi sympathizers formed the underpinnings of the agency's dual mission.[238]

In the following years, and under the direction of long-serving Director J. Edgar Hoover, the FBI grew and expanded its investigative mission to include all federal crimes not specifically authorized to another federal agency, as well as all domestic national security operations.[239] Through many investigative successes, the FBI developed a worldwide reputation for cutting edge law enforcement techniques while apprehending bank robbers, mafia figures, kidnappers and foreign spies. These successes positioned the FBI to continue to grow while attaining additional investigative authorities. During this time period, the agency concentrated the majority of its resources on criminal investigations, with little emphasis on intelligence collection.

With the onset of World War II and the expansion of regimes deemed threatening to American democracy, Director Hoover directed his agents to investigate any activities which he designated a subversive act or a threat to the nation's security. Reportedly, during this time period, the FBI greatly enhanced its use of domestic wire-tapping, surreptitious interception and documentation of citizens' communications, and cataloguing of citizens' "subversive" activities.[240] By the passage of the National

236 "This Day in History, July 26, 1908, FBI Founded," History.com, accessed September 26, 2014, http://www.history.com/this-day-in-history/fbi-founded.

237 Ibid.

238 Ibid.

239 U.S. Federal Bureau of Investigation (FBI), *The FBI: A Centennial History, 1908–2008*, 2nd ed. (Washington, DC: U.S. Government Printing Office, 2008), http://www.fbi.gov/about-us/history/a-centennial-history.

240 "This Day in History, July 26, 1908, FBI Founded."

Security Act of 1947, the government had formally recognized that the Intelligence Community (IC) included externally facing military and intelligence agencies as well as domestically aligned investigative agencies led by the FBI.[241] During these years, the Bureau's intelligence collection mission became the agency's primary mission, a move that positioned the agency to receive increased funding and additional expansion.

The post-war years through the 1950s, '60s, and '70s saw the rise of the perceived threat of the expansion of communism abroad. Through these times, the FBI continued to investigate criminal acts under its broad jurisdiction as well as to conduct domestic counter-intelligence operations targeting groups deemed subversive to this country, namely groups supporting communism. Unfortunately, during this time period, the nation was experiencing disruptive challenges to the historical norms of the society as it wrestled with racial and sexual equality, unpopular wars overseas, political corruption and the existential threat of nuclear war. During this time, Director Hoover initiated a program known as COINTELPRO, which utilized the FBI's national security and law enforcement authorities to conduct intelligence collection operations against members of legitimate groups, public figures and citizens in violation of existing laws and our citizens' constitutional rights.[242]

The June 1968, the Omnibus Crime Control and Safe Streets Act was passed in an effort to provide guidance to law enforcement in their duties and to curb the rising gun violence in the country. Of importance for the FBI, the Act provided large budget increases for the agency to expand its operations. Additionally, Title III of the Act recognized that government agencies, namely the FBI and NSA, had utilized wiretaps (SIGINT) inappropriately and violated the privacy rights of American citizens.[243] The Act also outlined the means, methods and judicial oversight that the government could employ domestically to monitor the communications of its citizens while still protecting innocent party's communication.[244] The Act recognized that the government's increasing

241 National Security Act, Pub. L. No. 80-253, 61 Stat. 495 (1947).

242 "This Day in History, July 26, 1908, FBI Founded."

243 Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (1968).

244 Ibid.

exploitation of communications and other technology could degrade the privacy rights of citizens if not subjected to proper oversight.

In response to the violations uncovered regarding COINTELPRO and other IC domestic intelligence activities, the bi-partisan Church Commission was initiated to investigate the violations by the government, recommend guidance, and pass legislation to ensure the values of our nation were protected.[245] Though the earlier section detailing civil rights violations by the NSA may indicate that the NSA was the only overreaching agency examined by the Church Commission, the FBI had also developed ways to blend its law enforcement and national security/ intelligence authorities and capabilities to violate citizens' civil rights through electronic and physical surveillance. At the outset of the hearings, the commission recognized that certain agencies, including the FBI, had authorities that were so extensive that they had to be clearly understood to judge if the intelligence community had to be reformed.[246] Additionally, the commission identified that no guiding policies existed to limit the FBI's domestic intelligence operations, a mission that the bureau had undertaken at the direction of Director Hoover and various Attorneys General (AG).[247] Because of the lack of formal guidelines, the commission based many of its findings on the core national values of civil liberty protection and separation of powers. Quoting former AG Stone in 1924, the commission voiced a fear of any agency that could become a secret police could abuse its powers and become uncontrollable.[248]

Specifically the commission noted that the FBI had secretly intercepted written communications and opened more than 100,000 first class letters to develop files and investigations on an undocumented number of Americans with no proof of wrongdoing although those citizens had been designated by the agency to be "rounded up" in the event of an undefined "national emergency."[249] The commission also noted that FBI

245 "Final Report S. Rep No.94-755."

246 Ibid.

247 Ibid.

248 Ibid.

249 Ibid.

counterintelligence (CI) managers felt that existing laws and court decisions had "tied their hands" and decreased their ability to be effective against national security threats. According to one senior FBI official, the Bureau believed that breaking the law and violating citizens' rights was justified because the national security of the nation demanded it.[250] The commission declared that COINTELPRO and the actions of the IC "indisputably degraded our free society."[251] Finally, the commission recommended that only the FBI, with strict judicial oversight, would be authorized to conduct domestic intelligence activities including surveillance, electronic interception of communications, and the physical monitoring of foreign agents, and that those activities should never hamper criminal investigations which were the proper method to deal with domestic espionage conducted by foreign actors.[252]

The Church Commission, which issued its findings in 1976 shortly after the death of Director Hoover, caused sweeping changes within the FBI in its domestic intelligence operations. The commission's findings prompted then AG Levin to issue the first formalized guidance to the FBI regarding how it should conduct its domestic intelligence operations. Notably, the agency was required to certify that a targeted individual or group was radicalized and involved in breaking the law or violent criminality rather than mere suspicion.[253] These guidelines are credited as the reason that between 1973 and 1976, the number of FBI domestic security investigations dropped from over 21,000 cases to just 626.[254]

In 1978, the passage of the FISA Act, with its clear definition of electronic surveillance and interception, and the establishment of the FISA court to review domestic electronic surveillance operations conducted by the FBI, seemed to ensure citizens' civil liberties would be secure into the future.[255] The requirement that all operations be

250 Ibid..

251 Ibid.

252 Ibid.

253 FBI, *The FBI: A Centennial History*, 81.

254 Ibid.

255 *Foreign Intelligence Surveillance Act of 1978*.

authorized by a panel of judges and only target foreign intelligence targets ensured that domestic operations would continue to be conducted by law enforcement agencies in compliance within existing interception laws but, as developments in technology, communication methods and interception capabilities continued, the application of the existing laws struggled to adapt.

President Reagan's 1981 issuance of EO 12333 further defined the collection responsibilities of the IC, mandated that the FBI was the sole agency authorized to conduct domestic intelligence activities, and protected our citizens' civil liberties from abuse by government actions.[256] The EO mandated that any domestic collection missions undertaken by the FBI be within the guidance of the AG to ensure operational personnel received proper oversight and operated within established lawful guidelines.[257]

The 1984 passage of the Comprehensive Crime Control Act represented the government's growing awareness of the developing cyber world and the possibility that criminals could leverage it to commit crimes. This Act was also the first comprehensive revision of the U.S. Criminal Code since the early 1900s and contained provisions to account for the increasing use of technology in our daily lives.[258] Although the Act explicitly authorized the U.S. Secret Service to investigate credit card and computer fraud, the FBI's broad investigative authorities granted under Title 28, section 533 to also positioned the agency to develop an expertise in computer crimes.[259] The Act designated the improper accessing of a protected computer system a violation of federal law under Title 18 USC 1030.[260]

---

256 Exec. Order 12333.

257 Ibid.

258 Wikipedia, s.v. "Comprehensive Crime Control Act of 1984," accessed May 29, 2014, http://en.wikipedia.org/w/index.php?title=Comprehensive_Crime_Control_Act_of_1984&oldid=569528576.

259 28 U.S.C. 533–Investigative and Other Officials; Appointment, United States Code, vol. Title 28 USC 533, 2012, http://www.gpo.gov/fdsys/granule/USCODE-2011-title28/USCODE-2011-title28-partII-chap33-sec533/content-detail.html.

260 18 U.S.C. 1030–Fraud and Related Activity in Connection with Computers, U.S. Criminal Code, vol. Title 18, 1984, http://www.gpo.gov/fdsys/granule/USCODE-2010-title18/USCODE-2010-title18-partI-chap47-sec1030/content-detail.html.

The disintegration of the Soviet Union substantially decreased the Bureau's counter-intelligence mission and the agency's law enforcement mission again took precedence in resource allocation. To respond to the nation's increasing emphasis on stemming the flow of drugs into the country and the threat posed by organized crime, the bureau re-established itself as the nation's leading law enforcement agency. Throughout the 1980s and '90s, international terrorism was generally perceived by the American public to be a threat to our citizens in other parts of the world with few acts or threats being identified domestically. In response to attacks against our citizens and military overseas, FBI Director Webster made counterterrorism the fourth national priority and, in the following years, many investigations involving attacks against Americans overseas were undertaken by the Bureau.[261] Following the first terror attack against the World Trade Center in 1993, then FBI Director Freeh identified that terrorism was a major threat to our national security however; the Bureau continued to allocate the majority of its resources to traditional criminal investigations and approached terrorism in a de-centralized fashion.[262]

As described elsewhere in this thesis, the 9/11 terror attacks caused widespread panic and demands on the government to ensure our citizens' security. In the days immediately following the attacks of 9/11, the Bush administration codified the changes that he had indicated were neccesary in his public address following the attacks. These early efforts also resulted in sweeping organizational and targeting changes for the U.S. intelligence program as well as the federal law enforcement community. For the FBI, the 9/11 attacks resulted in intense scrutiny and oversight as some felt that the agency had failed to protect the country by allocating too much of its resources towards reactive law enforcement activities while dminishing its national security responsibilties.[263] The post-9/11 scrutiny of the FBI rivaled the Church Commission/COINTELPRO period and

261 FBI, *The FBI: A Centennial History,* 82.

262 National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*, (Washington, DC: Government Printing Office, July 22, 2004), 93, http://govinfo.library.unt.edu/911/report/index.htm.

263 Ibid., 94.

forced the agency to concentrate its efforts on its counterterror and national security missions with less resources being allocated toward criminal investigation.

As described earlier, the passage of the USA Patriot Act continued the sweeping changes to the operational and legal guidance for both law enforcement and the intelligence community. As reported by Jaeger, Bertot and McClure, the ‘s changes to FISA requirements and other guidelines for the FBI, with its unique law enforcement and national security missions, resulted in changes which are still developing a decade later.[264] Most notably, Section 206 and 207, expanded the definition of "foreign power or intelligence" to include U.S. citizens if the government felt that they were affiliated with a foreign power, thereby removing any FISA protections for U.S. citizens.[265] Additionally, the target of the investigation or intelligence operation no longer needed to be involved in a violation of federal law and any information gathered could be shared with law enforcement and intelligence agencies.[266] The increased sharing between law enforcement agencies, operating under laws designed to ensure our citizens' privacy, and intelligence agencies focused on foreign actors with no privacy considerations, instantly removed Church Commission era prohibitions designed to protect U.S. civil liberties.[267] This prohibition on sharing between law enforcement and intelligence was commonly referred to as "the wall." Additionally, as reported elsewhere, Section 814 approved the application of 18 USC 1030 (CFAA Act) to acts of "cyber terrorism" although the definition required the loss of one life due to the act.[268]

In 2002, the FBI, recognizing that the rapidly developing cyber world formed the foundation of the nation's critical infrastructures and were susceptible to cyber attack or cyber terrorism; formed a dedicated Cyber Division to integrate the national security and

---

[264] Jaeger, Bertot, and McClure, "The Impact of the USA Patriot Act on Collection and Analysis of Personal Information."

[265] USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[266] Jaeger, Bertot, and McClure, "The Impact of the USA Patriot Act on Collection and Analysis of Personal Information," 7.

[267] Ibid., 7.

[268] USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

cyber investigative missions into a unified methodology.[269] The blending of the Bureau's national security and criminal investigative missions was evident in the Cyber Division mission statement to combat cyber-terrorism, hostile foreign intelllignce action conducted over the Internet, and cyber crime.[270] Additionally, the FBI initiated a cyber-specific agent training program to ensure its worlforce was prepared to operate effectively in the cyber world.[271]

As refererenced earlier in this thesis, the 2003 release of the President's National Strategy to Secure Cyber Space contained many mandates which indicated the government's growing awareness of the cyber threats facing the nation. Specifically for the FBI, the Strategy indicated that the FBI and DoJ lead the national effort to investigate and prosecute cyber crime.[272] Although the Strategy recognized that many cyber attacks are crimes, it indicated that national security and law enforcement must play a role in the nation's cyber-security stance but that law enforcement action offered the best opportunity to identify and apprehend the responsible attacker.[273] Finally, the Strategy called on the FBI to adopt an "Intelligence Led Policing" model to proactively identify and disrupt criminal, intelligence or counter-intellligence cyber operations in the U.S..[274]

In 2004, the long awaited 9/11 Commission Report was released. The report identified failures in the government's preparedness and response to the 9/11 attacks. Although the IC was collectively condemned for failing to successfully identify the terrorist's intent to attack the U.S. homeland, the FBI was widely criticized for having a lack of imagination to envision the terrorist's plans.[275] The Report identified that the FBI's National Security structure was designed for Cold War threats and as unprepared to

269 "Ten Years after 9/11–Cyber," *FBI.gov*, May 19, 2014, http://www.fbi.gov/about-us/ten-years-after-the-fbi-since-9-11/just-the-facts-1.

270 Ibid.

271 Ibid.

272 Bush, "National Strategy to Secure Cyberspace."

273 Ibid,43.

274 Ibid,74.

275 National Commission on Terrorist Attacks, *9/11 Report*, 339.

counter the threat posed by terrorism.[276] Additional allegations noted in the report include that the FBI lacked the ability to collect information gleaned in field office investigations, and was operating as an investigative entity more interested in prosecutions of past attacks than an intelligence collection agency seeking to thwart an attack.[277] The report further called on FBI to re-allocate personnel to develop a national security workforce which was to concentrate specifically on intelligence and national security issues resulting from terrorism.[278] Finally, the Report spent considerable effort identifying the inability of law enforcement information to be shared with the IC as a primary reason that the terrorist plot was not identified and interupted.

Following quickly behind the Commission report, The Intelligence Reform and Terrorism Prevention Act of 2004 required the national security mission of the FBI to take precedence over the criminal investigative responsibilities. The Act required all agents to receive mandatory counter-intelligence training and to be designated as certified intelligence officers.[279] Additionally, the agency was required to allocate large portions of its budget to intelligence and counter-terror activities while designating intelligence specific career tracks for personnel who would not be required to be invovled in the agency's traditional criminal investigative core mission.[280]

In 2008, Attorney General Mukasey issued sweeping new guidelines, referred to as the Mukasey Guidelines, to guide the agency's operations and new, national security centric role.[281] According to the guidelines, the separation of criminal and national security cases and information, and the designation of personnel as counter-

---

276 Ibid., 416.

277 Thomas Keane and Lee Hamilton, *9/11 Commission Report– Executive Summary*, National Commission on Terrorist Attacks upon the United States (National Commission on Terrorist Attacks upon the United States, July 22, 2004), 18, http://govinfo.library.unt.edu/911/report/911Report_Exec.htm.

278 Ibid., 31.

279 Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004).

280 Ibid..

281 Jerome P. Bjelopera and Mark A. Randol, *The Federal Bureau of Investigation and Terrorism Investigations* (CRS Report No. R41780) (Washington, DC: Congressional Research Service, January 14, 2013), http://assets.opencrs.com/rpts/R41780_20110427.pdf.

terror/intelligence or criminal investigators would be discontinued.[282] The guidelines also designated computer intrusions conducted by foreign entities, and not necessarily foreign governments, to be designated and investigated as a national security issue.[283] The mandatory sharing of criminal investigative information and evidence with classified information and intelligence agencies represented the final step over the Church Commission "wall" which had existed to protect the privacy of the public and was resisted by many in the criminal investigations field. The removal of the wall was also unsettling to many civil liberties groups who believed that the role of the judiciary and law enforcement would be diminished in relation to intelligence and counter-intelligence requirements and that intelligence investigative authorities would be utilized to by-pass normal criminal procedures designed to protect citizens' civil liberties.[284]

In the FBI Cyber Division, the "over the wall" sharing authorized by the Patriot Act, encouraged by the 9/11 Commission, and mandated by the AG was evident in the creation of the FBI administered National Cyber Investigative Joint Task Force (NCIJTF) which was incorporated into the 2008 release of the CNCI.[285] The NCIJTF was envisioned to serve as a multi-agency national focal point for counter-intelligence, intelligence, counter-terrorism and law enforcement cyber operations to quickly integrate and share cyber threat related information.[286] The CNCI identified that many security experts were concerned that hostile cyber actors would progress from committing crimes online to taking actions that would disrupt or destroy cyber supported critical infrastructures such as telecommunications or the financial services sector through the deployment of undefined cyber weapons.[287]

As this section indicates, throughout its history the FBI successfully endured many periods of operational success followed by allegations of overreach and intense

---

[282] U.S. Department of Justice (DOJ), *Attorney General's Guidelines for Domestic FBI Operations* (Washington, DC: DOJ, September 29, 2008), 5.

[283] Ibid., 7.

[284] Bjelopera and Randol, *The Federal Bureau of Investigation and Terrorism Investigations*, 12.

[285] "Ten Years after 9/11–Cyber."

[286] Ibid.

[287] Rollins and Henning, *Comprehensive National Cybersecurity Initiative*, 6.

scrutiny resulting in re-organization or resource re-allocation. The decade after the 9/11 attacks represents the most recent time period for the agency as it refocused its resources and efforts from reactive traditional criminal investigations, to intelligence driven counter-terror or national security efforts, and finally towards the developing cyber world. As reflected in a website detailing the FBI's changing focus in the post-9/11 decade, the Bureau changed from a case based, law enforcement-centric contributor to the IC, to a hybrid law enforcement/national security, threat driven, full IC partner focusing on terrorism and cyber threats.[288] To accomplish this re-organization, the Bureau increased its staffing from approximately 27,000 employees to approximately 35,000 employees including a 200% increase in cyber trained personnel and intelligence analysts, while the agency's budget increased from approximately $3.8 billion USD to almost $9 billion.[289]

Perhaps the most effective indicators of the Bureau's increasing emphasis on cyber threats from its counter-intelligence and counter-terror focus are the statements of its leadership in the media and during Congressional testimony. In March 2012, then Director Robert Mueller was invited to provide the keynote address to the widely attended annual RSA Cyber Conference in San Francisco, CA. In this speech, Director Mueller emphasized the cyber threat from national security and state sponsored attackers, cyber terrorism, organized crime groups, and hacktivists.[290] Mueller also highlighted the detailed the growth of the NCIJTF and the FBI's recognition that, although terror was the agency's primary focus, cyber threats clearly represented the future top threat and priority for the agency and that success for the agency required the successful attribution of the attacks.[291]

---

288 "FBI: A Decade in Numbers," blog, *Emptywheel.net*, (September 14, 2011), http://www.emptywheel.net.

289 Ibid.

290 Robert Mueller, "Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies," *FBI*, March 1, 2012, http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

291 Ibid.

More recently, in May 2013, FBI Cyber Division Assistant Director (AD) Joseph Demarest emphasized the growing cyber threat to the U.S. critical infrastructure from foreign intelligence and nation-state sponsored actors, terrorism, organized crime and hacktivists during his testimony to the Senate Judiciary Subcommittee on Crime and Terrorism.[292] During this testimony, AD Demarest described the FBI's "NextGen Cyber" program that sought to prepare the agency for future cyber threats that would soon be the top issue for the agency. For evidence, AD Demarest described the agency's initiation of fully staffed and funded Cyber Task Forces (CTF) in each of the FBI's 56 Field Offices (FO) which were modeled after the successful FBI administered Joint Terror Task Force (JTTF) program; plans to expand the NCIJTF to include foreign law enforcement and intelligence agencies; and the deployment of a cyber intrusion reporting web portal known as "IGuardian" which was also modeled after the JTTF "Guardian" web portal.[293]

Shortly thereafter, in June 2013, FBI Executive Assistant Director (EAD) Richard McFeeley testified before the Senate Appropriations Committee regarding the preparations the agency was undertaking to prepare for future cyber threats. EAD McFeeley testified that, between 2002 and 2012, the FBI had experienced an 84% increase in intrusion investigations and followed with a funding request for 152 additional cyber-specific positions to help counter the growing threat.[294] Additionally, McFeeley described the interagency development of a formalized "lanes in the road" document for U.S. government cyber security operations detailing the roles and responsibilities of the NSA, FBI and DHS.[295]

Most recently, newly appointed FBI Director James Comey described the agency's perception of the threats faced by the country in his November 2013 testimony

---

292 Joseph Demarest, "Responding to the Cyber Threat," *FBI*, May 8, 2013, http://www.fbi.gov/news/testimony/responding-to-the-cyber-threat.

293 Ibid.

294 Richard McFeeley, "Cyber Security: Preparing for and Responding to the Enduring Threat," *FBI*, June 12, 2013, http://www.fbi.gov/news/testimony/cyber-security-preparing-for-and-responding-to-the-enduring-threat.

295 Ibid.

to the Senate Committee on Homeland Security and Governmental Affairs. Director Comey identified intelligence driven counter terrorism as the agency's primary mission but posited that, in the near future, the agency would be required to re-allocated the majority of its resources and budget to countering cyber threats as they became the most pervasive threat.[296] Director Comey also reported on the FBI's partnership with DHS and the NSA to co-chair the Enduring Security Framework (ESF) which sought to bring together the top leaders of private industry and the government to identify cyber threats issues and work together to counter those threats in the most effective method.[297]

As this section indicates, the history of the FBI includes many operational and organizational successes that positioned the agency to be the preeminent law enforcement and national security agency in the country. Between those successes however there have been instances of overreach and illegal behavior that resulted in Congressional scrutiny, reorganization or the redirection of the agency's mission. The decade after the 9/11 attacks represents the most recent time period for the agency as it refocused its resources and efforts from reactive, traditional criminal investigations to intelligence driven counter-terror or national security efforts and finally towards the understanding that the developing cyber world represented the future of all operations. With its broad authorities and capabilities, the FBI will represent an integral part of the government's cyber security effort into the future.

D. U.S. SECRET SERVICE

In 1806, due to the widespread counterfeiting of currency in the United States, which threatened the stability of the newly formed nation, counterfeit detection and suppression was delegated to the U.S. Marshals and district attorneys through the Enforcement of Counterfeiting Prevention Act.[298] In 1860, the responsibility for the nation's currency and financial infrastructure was transferred to the U.S. Treasury

296 James Comey, "Homeland Threats and the FBI's Response," *FBI*, November 14, 2013, http://www.fbi.gov/news/testimony/homeland-threats-and-the-fbis-response.

297 Ibid.

298 Shawn Reese, *U.S. Secret Service: An Examination and Analysis of Its Evolving Mission* (Washington, DC: Congressional Research Service, July 31, 2008), 8.

Department and, by 1862; the nation had adopted a unified national currency.[299] Shortly thereafter, in 1865, due to ineffective enforcement by the Marshals, the Secret Service Division (SSD) of the Treasury Department was formed to suppress the continued widespread counterfeiting of U.S. Currency, estimated at over one third of all currency in circulation, and to defend the nation's nascent financial infrastructure.[300] The SSD was very effective in its enforcement efforts, and in 1867, Congress authorized the SSD to investigate "frauds against the government" and other violations a directed.[301]

During those early years of operation, the SSD, which was renamed the U.S. Secret Service (USSS) after achieving stand-alone status within the Treasury Department, became the preferred agency to conduct a wide range of investigations, including espionage and smuggling, at the direction of the President and Congress. The agency, in line with its original mission, continued to specialize in financial crimes investigations as its core investigative mission.

In 1901, shortly after the assassination of President McKinley, the USSS was informally requested to provide protection for the U.S. President, a duty that was statutorily authorized in 1913 and for which the agency became most widely recognized.[302] Over the next 60 years, the USSS protective mission continued to expand to include U.S. Presidents and their families, Vice Presidents and their families, Presidential and Vice Presidential candidates, visiting foreign heads of state and others as authorize by executive order.[303] Also during this time, the agency's authority to conduct its diverse, yet complimentary, investigative and protective functions was codified under Title 18, Section 3056 of the United States Criminal Code (USC).[304]

---

299 "United States Secret Service: Criminal Investigations," United States Secret Service, accessed June 7, 2014, http://www.secretservice.gov/criminal.shtml.

300 Reese, *U.S. Secret Service: An Examination and Analysis*, 8.

301 "United States Secret Service: Criminal Investigations."

302 Ibid.

303 Ibid.

304 *18 U.S.C. 3056 - Powers, Authorities, and Duties of United States Secret Service, United States Criminal Code*, vol. 18, 2012, http://www.gpo.gov/fdsys/granule/USCODE-2011-title18/USCODE-2011-title18-partII-chap203-sec3056.

Throughout its history, regardless of the public's perception that the agency was predominantly an executive protection agency, the USSS continued to serve as the primary investigators of criminal violations against the nation's financial and banking systems through proactive investigations and leveraging technology as it developed. Although the agency periodically was requested to assist other law enforcement entities fulfill their missions, the USSS concentrated its efforts on developing a financial crimes investigation specialty, always with a goal of protecting the nation's financial infrastructure.

To address developing alternate payment systems, the Comprehensive Crime Control Act of 1984 extended the USSS's primary investigative authority to access device fraud (Title 18 USC 1029) and, in recognition of the effect developing technology would have on the nation's financial systems, Computer Fraud (Title 18 USC 1030).[305] Additionally, recognizing that statutes were required to account for cyber-supported crimes such as Distributed Denial of Service (DDoS) attacks, Congress passed the Computer Fraud and Abuse Act of 1986 (CFAA) which authorized the USSS concurrent investigative jurisdiction with the FBI for violation of Title 18 USC 1028 (identity theft), and Title 18 USC 1030 amendments classifying computer intrusions, and crimes committed against federally insured financial institutions.[306]

The passage of Title 18 USC 1030, and enforcement authorization being concurrently provided to the USSS and FBI, provided both agencies with very broad authority to investigate or respond to any cyber intrusion into any protected computer system. 18 USC 1030 has been designated as a "cyber security law….which protects federal computers, bank computers and computers connected to the Internet."[307] As both agency's developed their cyber investigative missions, this statute provided both with the authority to conduct cyber security activities in furtherance of both law enforcement and

305 "United States Secret Service: Criminal Investigations."

306 *Wikipedia*, s.v. "Computer Fraud and Abuse Act," accessed May 29, 2014, http://en.wikipedia.org/w/index.php?title=Computer_Fraud_and_Abuse_Act&oldid=610122220.

307 Charles Doyle, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws* (CRS Report R42659) (Washington, DC: Congressional Research Service, January 27, 2010), 2.

cyber protective missions far beyond the lawful capabilities of other cyber security entities.

Since the passage of the CFAA and, as cyber-enabled crimes continued to evolve, the USSS adapted its capabilities to account for changing technologies that threatened the nation's critical financial infrastructure. As the financial sector became more reliant on cyber technologies and the cyber-based threats became more pervasive, the USSS has consistently increased its investment in its cyber-investigative and protective capabilities. But by 1995, the USSS recognized that technology developments, and the rapid adoption of those technologies by the financial sector, would quickly outpace the agency's capability to achieve success. To account for this, the USSS developed a first-of-its-kind trusted partnership with the private sector, law enforcement, and academia in a task force approach to effectively share threat information, cyber intelligence and cyber security best practices. This model, which was quickly emulated throughout government, became known as the Electronic Crimes Task Force (ECTF) model.[308] Over the next six years, the ECTF became the hallmark of the agency's method of working in trusted partnership with the financial industry and other entities to fight cyber crime and protect the nation's critical infrastructures.

In 2001, the USSS was still aligned within the U.S. Treasury Department, where its financial crimes expertise and consistent, cutting-edge success in financial and cyber investigations were recognized. However, following the attacks of September 11, 2001, the U.S. government sought to re-organize their capability and re-establish the confidence of the American public. During this turbulent time, many new threats were identified and sweeping organizational changes were made to the government's operations and structure.

The USA Patriot Act, passed on October 26, 2001, called for the nationwide expansion of the USSS Electronic Crime Task Force (ECTF) model, which was identified as a successful method of investigating the terrorist use of cyber technologies and the prevention of attacks against the nation's financial infrastructure through

308 "About the U.S. Secret Service Electronic Crimes Task Forces," United States Secret Service, accessed June 8, 2014, http://www.secretservice.gov/ectf_about.shtml.

aggressive enforcement and information sharing among the trusted partners.[309] While the USSS worked to expand the ECTF network, it was also directed to utilize its expertise in physical protection combined with its cyber investigative specialties to provide support to other cyber-supported critical infrastructures. Within the financial sector however, portions of the that mandated widespread sharing of information gleaned from Secret Service investigations, and the corollary expansion of national security investigations, were met with resistance, as private industry perceived the government was seeking access to corporate data integral to their business model.

On November 25, 2002, in what would forever change the mission and duties of the USSS, the Department of Homeland Security (DHS) was formed with the passage the Homeland Security Act of 2002 (HSA), and the further passage of significant legislation to enable the homeland security mission.[310] Of importance for the USSS cyber mission, Title 18 USC 1030, which was rapidly becoming a core USSS violation, was amended to allow for a broader application of the "protected computer system" definition and for increased sentences due to the damage caused to the system.[311] However, most importantly for the USSS, through Subtitle C of the HSA, the function, personnel, assets and obligations of the Secret Service were transferred from the Secretary of the Treasury to the Secretary of Homeland Security although the HSA mandated that the USSS was to remain a distinct agency.[312]

As one of the 22 agencies re-aligned under the newly formed DHS, the USSS struggled to retain its identity and unique history while still adding value to the new department. Many within the USSS felt that the agency had been a valued member of the U.S. Treasury Department since the agency was formed in 1865, and resisted the re-alignment to a department that appeared to have limited interest in financial crime investigations and executive/dignitary protection. But, as shown during this thesis, portions of the department's rapidly evolving mission positioned the USSS and its cyber

309 USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

310Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002).

311 Ibid., 22.

312 Ibid., 90.

investigative and protective capabilities and authorities at the forefront of the growing departmental mission of cyber security operations.

Over the next decade, although little cyber investigative legislation was passed or required, the USSS continued to invest heavily in its cyber capabilities to support both its investigative and protective missions. As with the FBI, perhaps the most effective measure of the agency's growing cyber focus are the public statements of USSS and DHS leadership in both interviews and testimony.

On April 3, 2003, during a hearing titled: "Fighting Fraud: Improving Information Security," USSS Special Agent in Charge (SAIC) Tim Caddigan testified on the importance of the USSS cyber capabilities to protect the nation's financial infrastructure and information systems to the Committee on Financial Services.[313] Specifically, Caddigan referenced the service's concentration on protecting the nation's financial and critical infrastructures from cyber-based threats as well as specific successes the agency had accomplished in detecting and preventing attacks against the banking systems.[314] Caddigan also reported that the USSS had responded to the mandate of the Patriot Act to expand the NY ECTF model and had initiated eight ECTFs throughout the country to assist in the effort.[315] Caddigan further testified that the agency had developed the Critical Systems Protection Initiative (CSPI), which leveraged its cyber investigative trained personnel to utilize their knowledge of adversarial and malicious cyber activity in support of the agency's protective mission through the prevention of cyber attacks which could cause physical effects and affect the integrity of the USSS protective mission. According to Caddigan, the agency had successfully utilized CSPI to secure the 2002 Salt Lake Olympics.[316] Following this deployment, CSPI was recognized within both the

313 *Fighting Fraud: Improving Information Security: Joint Hearing Before the House Subcommittee on Financial Institutions And Consumer Credit of the Committee on Financial Services,* 108th Cong., 1 (2003) (statement of Tim Caddigan, Special Agent in Charge, Financial Crimes Division, United States Secret Service).

314 Ibid.

315 Ibid.

316 Ibid.

USSS and DHS as proof that the Service's financial crimes and cyber capabilities offered a scalable resource to assist DHS in securing the nation's critical infrastructure.

Shortly thereafter, on September 16, 2003, DHS Assistant Secretary for Infrastructure Protection (IP) Robert Liscouski testified before the Subcommittee on Cybersecurity, Science, and Research and Development, regarding DHS' newly formed National Cyber Security Division (NCSD) and the department's cyber security activities. In a contentious meeting which included allegations regarding DHS' lacking cyber security focus and the ineffectiveness of the United States Computer Emergency Response Team (U.S.-CERT), Liscouski acknowledged that DHS/NCSD was required to provide cyber security for the nation's critical infrastructure.[317] Additionally, Liscouski testified that although DHS may not have sufficient department-level protective authorities, through the USSS, the department's cyber and physical protection authorities were very broad.[318] Finally, in acknowledging that the USSS was the preeminent cyber financial crime experts, Liscouski agreed that DHS planned on relying on the USSS' cyber authorities and workforce to achieve success.[319]

On February 3, 2004, then USSS Director Ralph Basham testified before the House subcommittee on crime, terrorism, and homeland security in regards to the USSS integration into DHS cyber operations and the agency's cyber crime expansion. During his presentation, Basham testified that the agency's investigations had developed from counterfeit currency and bank frauds to cyber-supported crimes due to the prevalence of technology within the financial sector. Basham also claimed that the ECTF model had "revolutionized" the government's cyber response capabilities and that the USSS had expanded the ECTFs into 12 domestic locations.[320] Basham also identified that the USSS

317 *The Invisible Battleground: Hearing Before the Subcommittee on Cybersecurity, Science, and Research and Development of the House Select Committee on Homeland Security*, 108th Cong., 1 (2003) (statement of Department of Homeland Security Assistant Secretary for Infrastructure Protection Robert Liscouski).

318 Ibid.

319 Ibid.

320 *Law Enforcement Efforts within the Department of Homeland Security: Hearing Before the House Subcommittee on Crime, Terrorism and Homeland Security*, 108th Cong., 2 (2004) (statement of United States Secret Service Director W Ralph Basham).

cyber methodology, drawing on the agency's physical protection mission, focused on leveraging technology and the information uncovered during investigations to prevent additional attacks against the nation's critical infrastructures.[321]

In August 2004, the USSS National Threat Assessment Center (NTAC), in concert with the Carnegie Mellon University Cert Coordinating Center (CERT-CC), issued a study entitled "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector." In utilizing NTAC, which specializes in developing behavioral-based guidelines for the USSS protective mission, in the criminal realm, the USSS was increasing its investment into cyber technologies and capabilities as well as indicating the increasing importance cyber security represented to the agency. The study, considered to be the first of its kind, indicated that behavioral approaches and security techniques could be effective in lessening an entity's exposure to threats from the cyber world.[322] The findings included 1.) Most intrusions required little technical sophistication; 2.) Most intrusions were financially motivated; and 3.) Incidents were often uncovered by different entities but were rarely discovered by the victim.[323] The *Insider Threat Study* was highly regarded and provided the basis for many cyber security programs in the following years. Additionally, CERT-CC and NTAC have re-evaluated the findings on a bi-annual basis and re-issued new findings to assist industry in cyber security best practices.

Further proof of the USSS' cyber investigative expansion and concentration was evident when, on July 9, 2009, the USSS issued a joint press with the Italian National Police and the Postal Police announcing the creation of the first international ECTF in Rome, Italy, which was followed by the initiation of an ECTF based in London, England.[324]

---

321 Ibid.

322 Marisa R. Randazzo et al., *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector* (Pittsburgh, PA: Carnegie Melon Software Engineering Institute, 2005), 12.

323 Ibid., 8, 13, 17.

324 "United States Secret Service Signs Partnership Agreement with Italian Officials Establishing the First European Electronic Crimes Task Force," U.S. Secret Service, July 6, 2009, http://www.secretservice.gov/press/GPA05-09_EuropeanECTF.pdf.

On April 12, 2011, USSS Deputy Special Agent in Charge (DSAIC) Pablo Martinez testified before the Senate subcommittee on Crime and Terrorism regarding how the USSS cyber investigative function was integral to the DHS mission to secure the nation's cyber-supported CIKR. As proof of the importance that the USSS cyber mission represented to the department, Martinez referenced DHS's recent publishing of the 2010 *Quadrennial Homeland Security Review* (*QHSR*), which established a unified strategic framework for the cyber security goals of the department as well as the *QHSR*'s description of the affect cyber criminals could have on the CIKR.[325] Martinez also referenced the recognition within the government of the USSS's cyber capabilities had resulted in the USSS being requested for input into the President's Comprehensive National Cyber Security Initiative.[326] Evidence of the agency's substantial investment towards its cyber security mission was provided by Martinez's description of the agency's recent establishment of the National Computer Forensics Institute (NCFI) located in Hoover, Alabama. The NCFI was the nation's first cyber training facility dedicated to developing cyber investigative capabilities for the state and local law enforcement.[327] Finally, Martinez highlighted a recent USSS cyber investigation which had enabled the agency to identify, and protect, over 100 corporations targeted by a cybercrime syndicate.[328]

As referenced in this section, the Secret Service is one of the nation's oldest law enforcement agencies and has served as the primary defender of the nation's financial sector since its inception to suppress the rampant counterfeiting of U.S. currency. Although the agency is most widely known for its mission of protecting the U.S. President and others, the agency has consistently developed its investigative techniques to account for technology developments as they relate to the financial sector. With the agency's transfer to DHS, and the inclusion of the agency into the department's mission

325 *Cybersecurity and Data Protection in the Financial Sector: Hearing Before the Senate Committee on Banking, Housing, and Urban Affairs*, 112 Cong., 1 (2011) (statement of United States Secret Service Deputy Special Agent in Charge Pablo Martinez).

326 Ibid.

327 Ibid.

328 Ibid.

of securing the nation's CIKR from varied cyber threats, the agency distinguished itself as a leader in cyber security through proactive law enforcement actions and is positioned to provide DHS with a capable, highly trained workforce leveraging its very broad cyber security authorities.

THIS PAGE INTENTIONALLY LEFT BLANK

V. ANALYSIS OF THE IMPLICATIONS OF THE CURRENT STRATEGIES

Chapter IV recorded the evolution of the DHS cyber security mission and the department's gravitation to technology supported cyber defense and information sharing initiatives. There has been an organizational hesitation to utilizing DHS law enforcement agencies authorities as an integral part of the department's cyber security efforts. In addition, the development of the cyber security missions and focus of the NSA (inclusive of DOD/Cyber Command), FBI, and USSS, the four entities that possess the most comprehensive authorities within the cyber security and enforcement arena, were discussed.

Chapter V leverages the information in the earlier chapters to analyze the implications of the differing approaches to achieving comprehensive cyber security, and recommend effective policy proposals for future government cyber security efforts. Microsoft's Butler Lampson, in his 2004 article, "Computer security in the real world" describes cyber security programs as being focused on five primary cyber security strategies which seek to "isolate," "exclude," "restrict," "recover," or "punish" the attackers.[329] The analysis of the implications of the DHS, NSA/DOD, FBI and USSS cyber focus will be reviewed using these principles applied to defensive technology and offensive operations.

A. DHS NETWORK DEFENSIVE RELIANCE IMPLICATIONS

As evidenced in the preceding chapters, since the time of its inception, DHS has continuously developed from what was initially a terror prevention and natural disaster response agency, towards focusing on critical infrastructure protection, and currently, to its focus on cyber security and the protection of cyber–supported critical infrastructures. Throughout its short history, the department developed a reliance on technology-based solutions, outreach efforts, and internal operational units while displaying little regard for the authorities and capabilities of legacy component DHS agencies. Chapter III, the

[329] Lampson, "Computer Security in the Real World," 3.

Literature Review, presented academic information regarding the applicability and effectiveness of technology-centric cyber security preparations, but the department has increasingly been asked by Congress and the private sector to define the success of the overall DHS approach to cyber security and whether it offers a path forward for the government's overarching cyber stance.

As mandated by the Homeland Security Act, DHS is authorized to lead the effort to secure and increase the resilience of the nation's critical infrastructures from attack and natural disasters.[330] As described earlier in this thesis, the majority of the nation's identified critical infrastructure is privately owned and/or outside of the immediate control of DHS. Although the Department has attained a level of success regarding disaster recovery and resilience through the utilization of its component agencies, namely FEMA and the Coast Guard, it has been widely criticized for failing in its cyber security mission.[331] Interestingly, the department's disaster response and recovery success through the efforts of its legacy agencies appears to not be recognized by the department leadership as a model to emulate within its cyber security mission. As developed in this thesis, to this point the Department's cyber security efforts have focused on technology (intrusion detection and prevention system) development and reliance, information sharing with private sector infrastructure owners, and massive budget expenditures to develop new agencies or entities who's mission would be duplicative of pre-existing DHS component agencies while simultaneously blaming failures on the department's lack of authorities to control other government agency's actions.[332] As critical infrastructure becomes increasingly reliant on cyber technologies, the implications of DHS's policy decisions will affect the nation's future prosperity and success as the world's economies and populations become increasingly interconnected and

---

330 Sharon S. Gressle, *Homeland Security Act of 2002*: *Legislative History and Pagination Key* (Washington, DC: Congressional Research Service, 2002), http://digital.library.unt.edu/ark:/67531/metacrs7490/m1/1/high_res_d/RL31645_2002Nov26.pdf.

331 U.S. Government Accountability Office (GAO), *Critical Infrastructure Protection Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities: Report to Congressional Requesters*, (Washington, DC: Government Accountability Office, May 2005).

332 John Curran, "DHS OIG Chides Cyber Office Over Planning Deficiencies," *Cybersecurity Policy Report*, July 11, 2011.

interdependent. For these reasons alone, the shortcomings of the department's cyber security programs, and the impact, must be fully understood to effectively propose policies going forward.

As evidenced by available literature and the department's own publications, the development of cyber defensive technologies represents the lynchpin of the department's cyber security efforts for securing both governmental and private sector owned critical infrastructure. In contrast, Chapter III, the literature review, provided academic studies of the effectiveness of technology defenses that indicated that solely relying on technology might be a misguided allocation of resources for a variety of reasons. Most notably, a defender can never be assured of identifying every weakness in his defenses and must remain in a response and recovery mode whereas the attacker has unlimited time to carefully reconnoiter and possibly reconfigure a system to identify and exploit defensive deficiencies. Additionally, the attacker must only find one weakness while the defender must identify all system weaknesses, an unfair advantage to the attacker to be sure. In effect, the adage that an attacker who spends their time building a taller ladder can always defeat the highest defensive wall, perfectly describes the false sense of security that reliance on technology to provide comprehensive security for our nation's cyber-supported critical infrastructures provides.

Many recent reports support the claim that the development of defensive tools has never been able to keep pace with the attacker's development of attack tools and that cyber security efforts centralized on defense have steadily fallen further behind the attacker's efforts.[333] Cyber security experts generally agree that comprehensive security that develops defensive technology, in combination with people, processes that identify and deter the attacker, and effective information sharing partnerships, is the only method of realizing success in the protection of our nation's cyber supported critical

333 PwC, *2014 U.S. State of CyberCrime Survey* (London: PriceWaterhouseCoopers, June 2014), http://www.pwc.com/us/en/increasing-it-effectiveness/publications/2014-us-state-of-cybercrime.jhtml.

infrastructures.[334] In furthering the "ladder" premise, without the ability to keep the attacker from climbing the ladder through active disruption of their efforts or deterring their attempt in the first place, the attacker will, inevitably, breach the defensive wall.

As related in the literature review, the premise that the entire knowledge base of the government's cyber programs, including NSA/DOD cyber attack forces and their tools and tactics, would also be leveraged by DHS for defense is also a misguided theory since numerous academic articles demonstrate that the government's cyber attack forces have little to gain from identifying and supplying DHS with system weaknesses that they exploit when conducting their primary attack or espionage missions.[335] The competing mission sets would ensure that DHS systems defenders would be operating without the benefit of knowing the most effective attack tools and how to effectively defend against them.

For additional consideration, the cyber espionage activities of the NSA/DOD are designed to be undetectable by the targeted system defenders. Since NSA operations are conducted in secret, it is obvious that cyber attackers seeking to exploit our systems would not feel any overt deterrent effect from NSA's operation. Shifting into the DOD cyber activities, consideration must be given that any overt use of our military to counter-attack a foreign-based attacker may be deemed as an act of war or aggression by the host nation and lead to an escalating series of attack and counter-attacks targeting our infrastructures. These types of activity could be disastrous to our infrastructure and cause the destruction of basic service capabilities such as power, telecommunications and water supply.

Despite their undeniable counter-attack and proven effectiveness in conducting foreign directed espionage, the above issues indicate that the NSA/DOD cyber attack forces are not the entity that DHS should rely on to keep attackers from climbing over their defensive "wall." Developing a solely defensive posture relies on Lampson's

334 "Cybercrime Incidents, Associated Financial Costs Surge While Organizations Still Unprepared to Battle Threats According to 2014 U.S. State of Cybercrime Survey from PwC and CSO," *PwC*, May 28, 2014, http://www.pwc.com/us/en/press-releases/2014/cybercrime-incidents-associated-financial-costs-surge.jhtml.

335 Moore, Friedman, and Procaccia, "Would a 'Cyber Warrior' Protect Us?" 2

strategy of "isolating" the system weakness, "excluding " or "restricting" the attacker from the system, while continually preparing to "recover" from a successful attack. Unfortunately, Lampson's "punishment" strategy to deter the attacker from attempting to climb the ladder is unattainable within DHS's current defensive strategy or through surreptitious means. A deterrent factor can, however, be attained through using historical law enforcement authorities to determine culpability for illegal activities and subsequently prosecuting the attacker through internationally accepted judicial proceedings. As referenced earlier, Title 18 USC 1030 designates all cyber intrusions against protected systems as criminal acts in violation of U.S. federal law.[336] William Goodman in his article "Cyber Deterrence: Tougher in Theory than in Practice," identifies that deterrence has specific elements which include deterrent declarations, denial measures, penalty measures, credibility, fear and a cost/benefit analysis by the attacker.[337] In effect, if a prospective attacker believes that their actions have a reasonable probability to result in arrest and a long period of incarceration, the attacker may not believe that the potential benefit is worth the cost of attacking. Recognizing, however, that some cyber attackers will not be deterred and will choose to commit an attack against a protected cyber system, every successful apprehension and incarceration will increase the possibility of deterring future attackers. If DHS recognizes the importance of the deterrent effect, successful law enforcement operations must become cornerstone of the department's cyber security effort.

Moving away from the deterrence discussion, DHS has actively promoted the development of trusted partnerships and information sharing initiatives with the private sector given the private sector's ownership of the nation's critical infrastructure. Of importance to this effort is if the department is able to develop the requisite level of trust with the private sector and foster a partnership with system owners. Because of the department's reliance on defensive technology of questionable effectiveness that must be placed on, or within, privately owned systems, the department's motives have been

336 *18 U.S.C. 1030 - Fraud and Related Activity in Connection with Computers*.

337 Will Goodman, "Cyber Deterrence: Tougher in Theory Than in Practice?" *Strategic Studies Quarterly* (2010): 4.

viewed skeptically by the system owners. Research indicates that the department has found it difficult to remain current with the dynamic nature of the cyber threat landscape.[338] One of the most effective ways to develop the requisite level of trust and partnership with system owners is the effective sharing of actionable information between the government and private sector. Unfortunately, although some success has been achieved, many aspects of DHS's information sharing efforts have been criticized and slow to develop due to governmental difficulties in sharing classified threat reporting.[339]

In an effort to facilitate active information sharing, the department developed a network of "information sharing and analysis centers" (ISACs), with one of the first being the Financial Services-ISAC (FS-ISAC). The ISAC concept places critical infrastructure industry representatives at the department's National Cyber security and Communication Integration Center (NCCIC) and provides instantaneous cyber threat intelligence sharing with the partners through their representatives.[340] The NCCIC has been designated as the collection point for any cyber intelligence the department receives from the private sector, U.S. intelligence agencies, international CERT teams and law enforcement regarding current threats and attacks.[341] As this information is received, it is transmitted throughout the world to other private industry contacts, law enforcement, and over 200 worldwide CERT teams to strengthen worldwide cyber defenses. The NCCIC and ISAC system is a positive step towards information sharing and has been widely praised as one of the department's most effective efforts although it still periodically

338 U.S. Government Accountability Office (GAO), *Critical Infrastructure Protection Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities: Report to Congressional Requesters* (GAO-05-434) (Washington, DC: GAO, May 2005), 17.

339 U.S. Government Accountability Office (GAO), *Critical Infrastructure Protection: DHS Needs to Better Address Its Cybersecurity Responsibilities* (GAO-08-1157T) (Washington, DC: GAO, Sept. 16, 2008), http://www.gao.gov/products/GAO-08-1157T

340 Edwards, *Review of the Department of Homeland Security's Capability to Share Cyber Threat Information.*

341 *Facilitating Cyber Threat Information Sharing and Partnering with the Private Sector to Protect Critical Infrastructure: An Assessment of DHS Capabilities: Hearing Before Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies,* 113th Cong., 1 (2013) (statement of NPPD Office of Cybersecurity and Communications Acting Assistant Secretary Roberta Stempfley and National Cybersecurity and Communications Integration Center Director Larry Zelvin).

encounters problems when attempting to share classified threat information with system owners.[342] The inclusive manner that the NCCIC facilitates is obviously fostering an environment of partnership and represents a valuable path forward for the department and provides infrastructure owners with the ability to block many current threats and attacks.

The information sharing efforts are in line with Lampson's strategies of "isolating" and "restricting" the threat actor's capabilities to successfully attack the nation's cyber supported critical infrastructure while seeking the goal of making each private owner "accountable" for their system's "integrity" and "availability." As long as the NCCIC remains central to the department's information sharing efforts, the benefit the private sector realizes from being an active partner will ensure their ongoing interaction and cooperation. Failure to continually promote active information sharing between the government and private sector will allow the cyber security effort to revert back to individual system owners ineffectively attempting to defend their systems without awareness of the threat they are facing, the latest tools begin deployed against them, or the best practices discovered through attacks against other private system owners.

As referenced earlier, DHS's mandate to coordinate the government's cyber security and response efforts has been resisted by other government agencies involved in related, but often competing, cyber missions. Repeated calls from within the DHS, the private sector and independent cyber security researchers, to provide the department with authorizing legislation and the ability to force compliance have thus far been unsuccessful.[343] The government's refusal to provide the department with some method of forcing the compliance of the other agencies has, at times, relegated the department to "asking" for other agencies to assist in cyber security efforts and hindered the overall government cyber security effort.

Without considering the private sector ownership of the majority of the nation's supporting critical infrastructure, the U.S. government controls many cyber-supported

342 Wilshusen and Barkakati, *Cybersecurity*: *National Strategy, Roles, and Responsibilities.*

343 Ibid., 4.

systems that fall outside of the control of DHS and which are vitally important to the nation's prosperity including, the internal systems of the Department of the Treasury, Defense, Internal Revenue Service, and others. A successful cyber attack against one of those systems could cause cascading effects that would threaten the stability and integrity of the government systems and functions as well as the distrust of the system by our citizens. In recognition of the importance of the goal of securing our cyber-supported critical systems, the policy proposals later in this thesis will leverage DHS's current activities along with other activities being conducted by governmental cyber attack, law enforcement and intelligence agencies.

B. NSA/DOD CYBER SECURITY AND INTELLIGENCE IMPLICATIONS

As described in Chapter IV, the evolution of the NSA from an agency focused on the collection and exploitation of foreign adversary's communications (COMINT) to focusing on the exploitation of signals intelligence (SIGINT), has positioned the agency at the forefront of the nation's cyber security efforts resulting in the exponential growth of its structure and funding. The unique mission, structure, and capabilities of the agency, which operates as both a civilian intelligence (SIGINT) collection agency and a Department of Defense military organization (U.S. Cyber Command or CYBERCOM), provides the agency with opportunities to leverage the development of the Internet and cyberspace unmatched by any other U.S. government agency. The world's increasing reliance on Internet communications and the interconnected cyber supported infrastructures allowed the NSA to develop its influence within the government and private cyber-supported critical infrastructure systems. But NSA's development of cyber attack capabilities and domestic cyber security operations leaves the nation with a number of unresolved issues to include; whether the nation will allow the agency to have access to citizens' personal information from the Internet and private corporate systems, which could appear to be a violation of our citizens' right to privacy; and whether the nation should trust an intelligence agency to protect our civil liberties. Questions have also been raised regarding whether NSA domestic "information assurance" operations violate long held prohibitions restricting the use of the military and intelligence agencies within the homeland since NSA leadership is "dual hatted" as the Director of the NSA

and Commander of CYBERCOM. In light of these unresolved issues, various writers have indicated that the nation must decide if the domestic utilization of a military/intelligence agency is a violation of long-held American values?.

The rise of the NSA as, arguably, the government's primary cyber-security agency for the nation's critical infrastructures, has been swift in light of the restrictions periodically placed on the agency by numerous legislative bodies following well-documented abuses of its capabilities and lawful authorities.[344] One factor that undoubtedly assisted in the development of the agency's cyber-security focus and capabilities was the redefining of criminal or national security cyber activities to being indicators of the future "cyber war" or "cyber terror" campaign that the nation would undoubtedly face. Not surprisingly, given its significant SIGINT capabilities and rapidly developing cyber attack capabilities, NSA continues to market itself as the obvious, and only, choice in cyber security. According to NSA, the agency is perfectly positioned because it can serve as a deterrent or counter-attack force capable of successfully mitigating threatening attackers, in effect positioning itself to keep the attackers off the "ladder" and serving as a deterrence to future attacks. However, as described in the literature review, the agency's claims of future acts "cyber terror" and "cyber war" has been refuted by numerous scholars as an over blown threat. Detractors argue that, by definition, "cyber terror" and "cyber war" are not valid descriptions of the activities of cyber attackers since the effects of the attack would cause the effect terrorists or attacking military forces seek or require.[345] Scholars claim that the world has never experienced an act of cyber terrorism, and is unlikely to ever experience one because a cyber attack would not terrorize the population; instead the acts would merely disrupt modern conveniences. Additionally, due to the vastness of the Internet and the redundant systems common in our critical infrastructures, any cyber attack initiated by terrorists would not cause anything but minor disruptions in service that would be easily negated through technical means.

---

[344] O'Connell, "Cyber Security without Cyber War," 1.

[345] Gabriel Weimann, "Cyberterrorism: How Real Is the Threat?" (Washington, DC: United States Institute of Peace, 2009), http://dspace.cigilibrary.org/jspui/handle/123456789/15033.

Regarding the possibility of future cyber-warfare, history has shown that the limited disruptive cyber attacks utilized during regional conflicts have not been successful in debilitating the targeted systems to support military action although they have disrupted citizen services.[346] Dissenting opinions also point out that, while cyber activity may be utilized to support kinetic military action through the disruption of command and control structures and other cyber-supported systems in the future, any act committed solely in cyberspace does not qualify as an act of "cyber war" and offers military operations few tangible results.[347] As described in the previous section however, utilizing our military forces to retaliate for a cyber attack directed against our infrastructure requires careful consideration because another nation may consider our response an act of war even if that is not our intention.

The consistent warnings regarding future acts of cyber terrorism directed at our nation's critical infrastructures, and acts of cyber-war perpetrated against our national interests, have been supported by the defining of the cyberspace as the newest "war fighting" domain. Not surprisingly, these claims have found its most vocal proponents within the nation's military and intelligence apparatus.[348] Proponents have continued their calls to develop cyber warfare capabilities despite the fact that all independent cyber security surveys and reports indicate that the overwhelming majority of malicious cyber activity is financially-motivated criminal activity with a much smaller segment being described as nation-state directed espionage activities.[349] In response, NSA/CYBERCOM has been one of the most vocal proponents of designating cyberspace as a war-fighting domain in order to position itself as the only entity capable of commanding the space.[350]

A review of the literature regarding capabilities and methods of the cyber threat indicates the nation must resist the efforts to militarize cyberspace. The rush to militarize

346 O'Connell, "Cyber Security without Cyber War," 5.

347 Gartzke, "The Myth of Cyberwar," 2.

348 III, "Defending a New Domain," 3.

349 O'Connell, "Cyber Security without Cyber War," 5.

350 Libicki, "Cyberspace Is Not a Warfighting Domain," 13.

cyberspace, with its requisite strict controls and oversight, could limit the original intent behind the development of the Internet as a communication platform to facilitate the open exchange of ideas and information. Additionally, if the nation is currently under constant attack through cyberspace and it should be considered the newest war-fighting domain, under what rules, if any, should the military operate? As noted cyber expert Martin Libicki points out, under what rules, and through which actions, can the military "fire back"?[351] Others ask, if cyberspace is a borderless domain, owned by no authority, whose national "use of force" laws apply?[352] Underlying all of these questions is the importance of attribution for attacks. As referenced in Chapter III, societies have consistently utilized law enforcement authorities to maintain internal order and the military to maintain external order.[353] Before the proper response to a cyber attack can be decided upon, the attack must be attributed to a specific actor, unfortunately, should the military respond without valid attribution, our response to what may have been mere criminal activity could be viewed as an act of war.

Outside of the militarization of cyber space, NSA's positioning as the government's leading cyber security agency protecting our nation's critical infrastructure also holds implications for our citizens' constitutionally protected right to privacy which must be carefully considered for several reasons.

First, the utilization of a "dual hatted" military and intelligence agency to conduct domestic cyber security operations may violate long-standing prohibitions against utilizing the military except in very limited circumstances.[354] The prohibitions against military intervention in civilian affairs is based on our nation's core principle that the military, which operates at the direction of the executive branch of the government, exists to defend the nation against foreign threats and should never be used by the government to control the citizenry. This important principle, enacted in 1878, is known as the Posse

---

351 Ibid., 13.

352 O'Connell, "Cyber Security without Cyber War," 12.

353 Brenner, "At Light Speed," 5.

354 Tomisek, *Homeland Security: The New Role for Defense*, 6.

Comitatus Act and is now codified in federal law as Title 18 USC 1385.[355] To preserve our liberties, the responsibility of enforcing a legislated code of conduct for our citizens has been delegated to domestic law enforcement agencies, whose operations are consistently reviewed by the judicial branch of government. This consistent oversight and separation of responsibilities and powers ensures the protection of our citizens' right to privacy from government interference. Expanding the rules for the domestic utilization of the military must be carefully reviewed to ensure there is no degradation of our citizens' basic rights.

Secondly, and of particular concern, is the slow blurring of the restrictions on IC operations, the clever use of the "dual hatted" positioning of the NSA leadership, and the co-location of NSA and DOD cyber forces. In a 2010 interview, then NSA Director and CYBERCOM Commander, General Keith Alexander, admitted that CYBERCOM does not have the legal authority or justification to operate domestically or to assist in the defense of privately owned cyber-supported infrastructure, adding that only the White House could legislate that activity.[356] According to Alexander, CYBERCOM was only authorized to defend DOD networks or to wage offensive operations against foreign targets. However, in the same interview, the "dual hatted" Alexander described how NSA's Information Assurance directorate was actively engaged in helping secure government and domestically located private networks from cyber intrusion.[357] Given the co-location and close coordination of the CYBERCOM and NSA personnel and operations, is it prudent to trust that the information and access allowed to one entity will not be shared with their close allies in the office next door? Additionally, as mandated in the Church Commission, U.S. intelligence agencies are prohibited from operating domestically. The only agency authorized to engage in domestic intelligence collection,

355 Charles Doyle and Jennifer Elsea, *The Posse Comitatus Act and Related Matters: A Sketch*, (CRS Report No. R42659) (Washington, DC: Congressional Research Service, August 21, 2012), http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA462391.

356 Shachtman, "Military's Cyber Commander Swears: 'No Role' in Civilian Networks."

357 Ibid.

while ensuring that our citizens' constitutional rights are protected through judicial reviews and oversight, is the FBI.[358]

The nation must carefully consider the implications of allowing NSA/DOD to redefine their operational domain and mission focus. As described in the Chapter IV, throughout its history, despite consistently issuing policies and guidance proposing to protect civil liberties, the NSA, and the greater IC, has consistently exceeded its legal authorities and illegally collected the constitutionally protected communications from our citizens in the name of national security. The nation must recognize that the redefining of cyber space as a borderless domain is very appealing to the NSA specifically because it removes the long standing prohibitions that restricts the agency's activities, and allows it to gather intelligence through the exploitation of cyberspace and the worldwide Internet communications of American citizens. Additionally, as widely reported, the worldwide distribution of networks through which those communications travel has provided the NSA with collection opportunities outside of the nation's borders while still, arguably, operating in compliance with existing legislation and guidelines.[359]

Finally, to augment the previously described DHS defensive cyber security stance, consideration must be given to the desired effect in utilizing NSA/DOD as the primary cyber security apparatus to protect our cyber supported critical infrastructure. Only the uninformed, certainly not this writer, would deny the capabilities of the NSA in the cyber intelligence collection and cyber exploitation arena however; the use of these capabilities must be carefully measured for their desired outcomes and targeting.

To provide a deterrent effect that dissuades nation-state attacks against our critical infrastructure, CYBERCOM's cyber network attack (CNA) capacity, as an externally focused cyber military force reminiscent of the Cold War nuclear deterrence strategy, has few peers. When NSA is utilized to conduct surreptitious, foreign cyber espionage activities, few would argue against that as improper use of the agency and its capabilities. However, as widely reported, since the majority of attacks targeting the nation's

358 "Final Report S. Rep No.94-755."

359 Daniel Byman and Benjamin Wittes, "Reforming the NSA," *Foreign Affairs*, April 17, 2014, http://www.foreignaffairs.com/articles/141215/daniel-byman-and-benjamin-wittes/reforming-the-nsa.

infrastructure are criminal in nature, neither of these capabilities represents the proper tool that deters the majority of future attacks.[360] To return to the earlier "ladder" reference, only a visible response or force, whose activities support Lampson's strategy of accountability and punishment, will result in deterring an attacker from launching an attack or building the ladder to scale the defensive wall. The surreptitious nature of NSA's important foreign espionage activities, by design and definition, can't provide a deterrence factor and should not be the government's choice to augment DHS's defensive efforts however, the agency's capabilities in cyber espionage targeting foreign interests, and its ongoing preparations to counter possible future foreign military cyber attacks, must be integrated into our nation's cyber security efforts. The following two sections discuss the two agencies with the authorities and capabilities to attribute cyber attacks against our nation's critical infrastructure to specific actors and to keep those attackers from climbing over the metaphorical defensive wall.

C. FBI NATIONAL SECURITY INVESTIGATIONS IMPLICATIONS

As described in Chapter IV, the FBI has developed to become the most recognized law enforcement agency in the U.S. The FBI is unique among U.S. law enforcement agencies due to its dual mission of criminal investigations and national security (intelligence collection) activities, which have allowed the agency the opportunity to redirect its assets and efforts to counter the most pressing enforcement issues of the day. However, as described earlier, these dual, sometimes competing, missions have caused the agency difficulties in the proper allocation of resources, agency infighting and overreach of authority. This section will analyze the FBI's position as the preeminent, national-security focused, law enforcement agency and how its approach to responding to cyber attacks against the nation's critical infrastructure is an important national capability whose use has implications that will affect our economic prosperity and the security of our national critical infrastructure far into the future.

360 "2013 Data Breach Investigations Report," Verizon Enterprise Solutions, accessed September 29, 2013, http://www.verizonenterprise.com/DBIR/2013/.

The decade after the 9/11 attacks represents the most recent time period for the agency, as it refocused its resources and efforts from reactive, traditional criminal investigations to intelligence driven counter-terror or national security efforts and finally towards the understanding that the developing cyber world represented the future of operations and budgets. The changing nature of the FBI's mission and how the agency viewed its future was captured in FBI Director James Comey's previously described November 2013 testimony to the Senate Committee on Homeland Security and Governmental Affairs. During that testimony, Director Comey identified intelligence-driven counter terrorism as the agency's primary mission but announced that the agency was beginning the process of re-allocating its personnel and budget resources to countering cyber threats to the national infrastructure as that became the most pervasive threat to the country's prosperity.[361] As an indicator of this shift, Director Comey identified the FBI's partnership with DHS and the NSA to co-chair the Enduring Security Framework (ESF), a committee which brings together the top leaders of private industry and the government to identify cyber threat issues and work together to counter those threats through the utilization of counter intelligence methods and information.[362] But is the application of, or reliance on, national security investigations the most effective method of describing and mitigating the threat or merely an effective method that should be carefully applied when mitigating specific cyber attacks?

Supporting Director Comey's testimony, during the May 2013 testimony of FBI Assistant Director (AD) for Counter Intelligence, Randall Coleman, to the Senate Judiciary, Subcommittee on Crime and Terrorism, FBI leadership clearly indicated that the agency views financially motivated cyber crimes and cyber attacks against any of the nation's 16 critical infrastructures as a national security issue regardless of the motivation or sponsorship of the attacker. AD Coleman specifically outlined the FBI's intention to allocate the Bureau's counter-intelligence resources to investigate "economic espionage"

361 *Threats to the Homeland: Hearing Before the Senate Committee on Homeland Security and Governmental Affairs Federal Bureau of Investigation*, 113th Cong. (2013) (statement of James B. Comey, director of the Federal Bureau of Investigation), http://www.fbi.gov/news/testimony/homeland-threats-and-the-fbis-response.

362 Ibid.

and the theft of trade secrets from private corporations as a national security issue.[363] Coleman further explained that the FBI had commenced investigating corporate espionage cases in conjunction with the DOJ National Security Division's (NSD) Counter Espionage section.[364] The re-defining of the criminal activity previously identified as corporate espionage should be given closer consideration for the far-reaching effects it may have for a few reasons.

First, few would argue that the theft of corporate trade secrets from select critical infrastructure owners, namely the defense/industrial contractors or government agencies, by nation-state supported cyber attackers does not constitute a national security issue. Clearly, the theft of that information by foreign agents could negatively impact the government's ability to maintain our military superiority, national defense, or our government's international negotiating efforts. However, the theft of a corporation's private manufacturing processes or intellectual property, which represents a monetary interest or benefit primarily to the private corporation's investors and executive staff can hardly be considered a national security interest. If the blurring of the definition of nation security interest continues, and the well-being of every corporation becomes a national security issue, whose responsibility will the security of their systems be? Careful consideration of this application of the "national security" designation must be made as to whether it indemnifies the private sector for their cyber security stance or provides the intelligence community or military with an avenue to attempt to expand their operations domestically.

To assist in properly defining the threat and the cyber attacker's intent, Georgetown University's Forrest Hare, in his presentation to the 2012 International Conference on Cyber Conflict, offered the following definitions describing national security cyber attack boundaries. Hare identified that national security cyber attacks could be committed by either nation-state supported or organized non-state actors, but

363 *Combating Economic Espionage and Trade Secret Theft: Hearing Before the Senate Judiciary Subcommittee on Crime and Terrorism*, 113th Cong., 2 (2014) (statement of Randall Coleman, assistant director of the Counter Intelligence Division of the Federal Bureau of Investigation), http://www.fbi.gov/news/testimony/combating-economic-espionage-and-trade-secret-theft.

364 Ibid.

that they must; 1) seek to gain knowledge from information systems which contain knowledge of national security value or; 2.) Attack critical infrastructure systems to degrade or disrupt such systems to cause a national crisis.[365] I propose that the government should not desire, nor will it benefit from, the responsibility for ensuring the security of corporate networks for cyber threats that fall outside of these parameters. The true beneficiaries of the expansion of the definition of a national security attack could only be the agencies whose budgets are increasingly funded to counter the threat, namely the FBI, NSA or, in specific circumstances, the DOD.

The second reason that the redefining of cyber criminal activity should be carefully reviewed prior to incorporation into our national strategy is that the methods of successfully mitigating these criminal acts already exist. Few currently in government recognize that the theft of intellectual property is a legacy U.S. Customs enforced criminal violation whose investigation authority has been transferred to DHS's Immigration and Customs Enforcement, Homeland Security Investigations Agency (ICE-HSI). In the increasingly constricted budgetary environment, the duplication of enforcement efforts and activities is inefficient and duplicative. Additionally, the FBI currently devotes a majority of its cyber-trained workforce to the Cyber Criminal Division, which conducts criminal investigations of cyber intrusions against protected systems in violation of Title 18 USC 1030. As documented earlier in this thesis, the FBI shares concurrent jurisdiction with the U.S. Secret Service for violations of 18 USC 1030 and, like the USSS, has successfully investigated numerous criminally motivated cyber attackers located domestically and abroad. Like the USSS, the FBI Cyber Division conducts criminal investigations to collect evidence for use in criminal prosecutions in compliance with existing criminal evidentiary laws and is subject to judicial and defense counsel review. In the rush to re-classify cyber criminal acts as national security events, the tactics and capabilities of the FBI criminal investigations may become over shadowed

365 F. Hare, "The Significance of Attribution to Cyberspace Coercion: A Political Perspective," in *Proceedings of 2012 4th International Conference on Cyber Conflict*, eds. Christian Czosseck, Rain Ottis, and Katharina Ziolkowski (New York: IEEE, 2012), http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6243970.

by national security investigations, many of which develop into long term monitoring operations versus operations which seek to identify and punish the attackers.

Over the course of its history, the FBI developed a well-deserved reputation for aggressively investigating espionage in the physical world, especially during the Soviet Cold War era. The agency is very effective at monitoring suspected foreign intelligence agents and conducting nation security investigations with a goal of criminally charging individuals involved in espionage and the theft of information vital to the nation's security. During that time period, the Bureau utilized classified techniques, including electronic interception, surreptitious entries, and other activities to identify the foreign espionage actors, develop evidence, and criminally charge the perpetrators. Historically, few of these cases resulted in open court proceedings; instead, many operations resulted in expulsions of foreign agents involved in espionage. As related earlier, many cyber security experts stress the importance of developing a deterrent effect to dissuade attackers from attacking the nation's cyber-supported critical infrastructures. Hare identifies that nation state attackers, when targeting a potential victim that has an active defense, response and cyber investigative capability, may be easier to dissuade from conducting attacks than a financially-motivated criminal, patriot hacker or terrorist due to their motivations and the need to remain secretive.[366] Recently, the FBI has initiated the process of criminally charging, and publically identifying nation-state attackers seeking to steal national security information.[367] Although, given the remote possibility that the attackers will ever be tried and the typical deterrent effect may be limited, the public response from the Chinese government indicates that publically attributing attacks to nation state actors may offer some measurable effect.[368]

---

366 Ibid..

367 Ellen Nakashima and William Wan, "U.S. Announces First Charges against Foreign Country in Connection with Cyberspying," *Washington Post*, May 19, 2014, http://www.washingtonpost.com/world/national-security/us-to-announce-first-criminal-charges-against-foreign-country-for-cyberspying/2014/05/19/586c9992-df45-11e3-810f-764fe508b82d_story.html.

368 Jonathan Kaiman, "China Reacts Furiously to US Cyber-Espionage Charges," *The Guardian*, May 20, 2014, http://www.theguardian.com/world/2014/may/20/china-reacts-furiously-us-cyber-espionage-charges.

As discussed in the preceding section, following abuses of our citizens' constitutional rights by the IC during domestic intelligence operations, legislation was passed which solely authorized the FBI to conduct domestic intelligence collection with appropriate judicial oversight.[369] The drive to expand the designation of all cyber attacks against the nation's critical infrastructure as a national security issue and expand the definition of espionage or national security interests may quickly overwhelm the agency and result in missed opportunities to mitigate true national security cyber attacks. More importantly, the designation of all cyber attacks against the nation's critical infrastructure as a national security event may also enable other government agencies, namely the NSA/DOD to argue for an increased role in domestic operations, an activity which has resulted in abuses of our citizens' rights and is in violation of existing legal guidance.

Finally, reports regarding the government's cyber security efforts have consistently indicated the importance of sharing cyber threat information regarding the tactics, techniques, and procedures (TTPs) of attackers with the owners of the critical infrastructure cyber systems to aid in their defensive efforts.[370] Equally consistently, the government's information sharing efforts have been criticized as ineffective or incomplete because government intelligence agencies have classified the TTPs as "secret" (S) or "top secret" (TS) and the system owners are not authorized, nor capable, of receiving classified information.[371] The current effort by the intelligence community to classify all attacks against the critical infrastructure as a national security event will, by design, further exacerbate this issue and ensure the necessary information will never be provided to system owners.[372] In contrast, the sharing of cyber criminal TTPs does not require S or TS classified access, is regularly shared with system owner/operators to aid

369"Final Report S. Rep No.94-755."

370 GAO, *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities.*

371 Edwards, *Review of the Department of Homeland Security's Capability to Share Cyber Threat Information,* 18.

372 Ibid., 20.

in their defenses, and has been recognized as a highly effective information sharing effort.[373]

Given the FBI's capabilities and authorities in conducting both criminal and national security cyber investigations, the agency should be integral to the nation's cyber security efforts. The agency's capabilities to conduct successful criminal investigations and prosecutions will compound the deterrent effects of other agency's efforts and supports defensive efforts to keep cyber attackers from climbing the "ladder" over DHS and private sector technical defenses. In addition, the agency's sole authorities to conduct domestic national security investigations allows the agency to utilize information received from the IC and its own intelligence investigations to attribute and publically charge nation-state supported attackers while still protecting our citizens' constitutional rights. The current attempts to re-designate all cyber attacks as national security events and the definition of the cyber world as a "borderless" domain can reasonably be expected to eventually impact the effectiveness of law enforcement operations, the privacy of our citizens' rights, and the effectiveness of the FBI's domestic counter-intelligence efforts as the IC chooses to instead conduct their own domestic operations. The efforts of the FBI, which has recently recognized the importance of disrupting national security attacks through investigations, versus of the historical IC method of passive monitoring, must remain a major part of the government's cyber security effort while still leveraging other agencies and their capabilities.[374]

D. U.S. SECRET SERVICE CRIMINAL INVESTIGATION IMPLICATIONS

As documented in Chapter IV, the Secret Service is one of the nation's oldest law enforcement agencies and has served as the primary defender of the nation's financial sector since its inception to suppress the rampant counterfeiting of U.S. currency. Although the agency is most widely known for its mission of protecting the U.S.

---

373 *Hacked Off: Helping Law Enforcement Protect Private Financial Information: Hearing Before the House Committee on Financial Service*s, 112th Cong., 1 (2011), (statement of Alvin T. Smith, Assistant Director, Office of Investigations, United States Secret Service), http://www.dhs.gov/news/2011/06/29/ testimony-assistant-director-smith-office-investigations-us-secret-service-house.

374 "FBI, Industry Fighting Back Against Cyber Attackers, Agency Official Says," *Defense Daily International*, June 13, 2013.

President and others, the agency has consistently developed its investigative techniques to account for technology developments as they relate to the financial sector. Following the agency's transfer to DHS, and the inclusion of the agency into the department's mission of securing the nation's CIKR from cyber threats, the USSS has distinguished itself as a leader in cyber-crime law enforcement through strategic and proactive law enforcement investigations targeting the most prolific, financially-motivated criminal cyber attackers in the world. Through these investigations, and an investment in its personnel, the agency had developed a highly trained workforce which is adept at leveraging its very broad cyber security authorities and is capable of providing DHS with an offensive capability that provides a deterrent effect to support the department's defensive efforts. This section will analyze the efforts and successes of the USSS cyber investigative activities and the implications of those activities being integrated by the department to support the DHS cyber security mission. It is noted that the previously discussed attributes of the FBI cyber crime investigations and their effect on the overall cyber security stance of the government applies to the USSS investigations however, USSS criminal investigations offer DHS addition benefits because the USSS is a component DHS agency.

As earlier described, the USSS shares concurrent jurisdiction with the FBI to investigate violations of Title 18 USC 1030 regarding cyber intrusions into protected systems.[375] Although the USSS has historically concentrated its investigative efforts to investigate intrusions targeting the nation's financial payment systems, the USA Patriot Act authorized the agency to conduct criminal investigations involving cyber intrusions supporting terrorism and to expand its network of ECTFs.[376] As the only DHS law enforcement agency with jurisdiction to investigate cyber intrusions, utilizing the USSS authorities and capabilities would provide DHS with an "in-house" offensive capability to deny attackers from using the euphemistic "ladder" to climb over the department's defensive walls. Supporting Lampson's description of comprehensive cyber security, USSS law enforcement operations provide DHS with the capacity to successfully "attribute" the cyber attacks to specific actors as well as to "isolate" and "punish" the

375 Doyle, *Cybercrime: An Overview of the Federal Computer Fraud.*

376 USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

attacker.[377] The well-documented deterrent effect recognized from arresting and incarcerating attackers can only serve to augment and support the defensive technology currently utilized by the department.

An additional effect of DHS effectively utilizing the USSS cyber investigative capability involves the ability for the department to utilize the USSS as its primary cyber response component when a cyber attack against the critical infrastructure is detected. As demonstrated earlier in this thesis and through DHS documents such as 2010's "Preventing and Defending against Cyber Attacks," the department has preferred to concentrate on defensive technology and publicized its reliance on its own cyber response capability in the form of the U.S.-CERT and ICS-CERT teams, while omitting the cyber response capability of the USSS.[378] Unfortunately, the CERT teams, while highly trained and technically capable, are predominantly located at DHS headquarters in Washington, DC, and lack the capacity to respond to the victim in the immediate aftermath of an attack and render aid if the victim requests on-site support, mitigation and DHS representation. Additionally, the CERT teams, and all other DHS response teams, lack the legal authorities of the USSS to respond to the victim location, initiate an investigation, mitigate the attack, and identify and apprehend the attacker.[379] Often, in the past, the department has been relegated to asking the FBI to respond to the victim and share whatever information the FBI discovers during its investigation. The USSS currently operates 45 field offices and 35 Electronic Crimes Task Forces (ECTF) that are located within two hours of all of the national critical infrastructures.[380] The distribution of USSS trained cyber-criminal investigators throughout the country offers the department the opportunity to provide a departmental cyber incident response capability that is unattainable through other internal DHS means.

---

377 Lampson, "Computer Security in the Real World," 4.

378 "Preventing and Defending against Cyber Attacks."

379 DHS and OIG, *U.S. Computer Emergency Readiness Team Makes Progress, 9*.

380 "About the U.S. Secret Service Electronic Crimes Task Forces," United States Secret Service, accessed June 8, 2014, http://www.secretservice.gov/ectf_about.shtml.

As described in the section detailing DHS' cyber security defensive efforts, one of the most successful operations of the department entails its ability to share cyber threat information with system owners to assist in securing their systems. Although not fully successful, the department's NCCIC has developed aggressively and is becoming widely recognized for providing actionable cyber threat information. Currently lacking its own primary collection capabilities, the NCCIC receives threat information from a network of international CERT teams, system owners and the IC community as it becomes available or is shared by the originators. Law enforcement techniques utilized by the USSS during its investigations, including long-term undercover operations, confidential informants, court ordered (Title III) communication intercepts and evidence collected through search warrants and subpoenas, offer the department an avenue of cyber-threat intelligence collection that has been relatively underutilized thus far. The leveraging of USSS derived evidentiary information may offer the department the opportunity to develop its reputation as the originator of cyber threat information and not be reliant on other agencies whose competing interests may impact the sharing effort.

Additionally, the evidence collected during active USSS investigations is often an optimal source of current cyber threat TTPs since it is derived directly from real-time law enforcement operations and current intrusions while still protecting the victim's identity. As related in the April 2014 Senate testimony of USSS Deputy Special Agent in Charge (DSAIC) William Noonan, proactive law enforcement operations often provide the USSS with information regarding ongoing, or planned, network intrusions not identified by any other method or source, including discovery by the victim.[381] DSAIC Noonan testified that, recognizing the importance of preventing or quickly mitigating an attack, the USSS supports utilizing the NCCIC to quickly share the information to critical system owners and worldwide cyber security teams.[382]

---

381 *Data Breach on the Rise: Protecting Personal Information from Harm: Hearing Before the Senate Committee on Homeland Security and Governmental Affairs*, 113th Cong, 2 (2014) (statement of USSS Criminal Investigative Division Deputy Special Agent in Charge William Noonan), https://www.hsdl.org/?view&did=753272.

382 Ibid.

The final implication of DHS utilizing information and access derived during USSS criminal investigations is that the department can openly report to system owners that their private corporate information, personnel identifying information, or other sensitive information will not be exposed to members of the IC or other private corporations through USSS investigations of NCCIC information sharing efforts. Both the USSS and the NCCIC have worked diligently to foster trusted partnerships with the private sector that stress discretion and privacy protection.[383] Following the revelations by former NSA employee Edward Snowden, regarding the NSA's widespread electronic surveillance of citizens' private communications and intrusions into private corporate networks, many system owners have become hesitant to allow government access into their private networks.[384] This hesitance by system owners may provide an opportunity to solidify the USSS and NCCIC as the government's primary cyber response and information sharing cyber security effort.

The Secret Service has developed a recognized expertise in conducting cyber crime investigations that represents a capability unavailable to the department through any other DHS component agency. The agency's legal authorities, cyber response and investigation, attack mitigation, criminal intelligence collection and deterrence capabilities can successfully fulfill missing cyber security capability gaps for DHS as it seeks to protect our nation's cyber-supported critical infrastructures. In the following section, recommended effective policy proposals for future government comprehensive cyber security efforts that leverage agency specific capabilities and authorities will be proposed.

383 *Protecting Consumer Information: Can Data Breaches Be Prevented?*: *Hearing Before the House Subcommittee on Commerce, Manufacturing and Trade*, 113th Cong., 2 (2014) (statement of USSS Criminal Investigative Division Deputy Special Agent in Charge William Noonan), https://www.hsdl.org/?view&did=750769.

384 Byman and Wittes, "Reforming the NSA."

VI. CONCLUSIONS, POLICY RECOMMENDATIONS AND FUTURE EFFORTS

The thesis reviewed available literature and evidence to offer answers to the stated research questions and provide a basis for effective policy recommendations.

- **Primary research question**: What strategies can the U.S. government develop that support the efforts of DHS, in concert with other governmental cyber security entities, to ensure the nation's cyber-supported critical infrastructure is provided with the most comprehensive security, while ensuring our citizens' privacy and security are preserved?
- **Secondary research question**: How could the application of established law enforcement investigative authorities and capabilities augment the technology-centric, defensive cyber methods currently utilized by the Department of Homeland Security to secure the nation's critical infrastructure against criminal cyber intrusions?

A. CONCLUSIONS

The thesis examined the U.S. government's post-9/11 initial focus on the threat posed by international terrorism to its shifting focus on the nation's resiliency to "all hazards" threats. The nation's subsequent recognition that the rapidly developing cyber world supports all of the nation's critical infrastructures and exposes vulnerabilities that could result in cascading effects and catastrophic results if exploited was then reviewed in this effort. As the department whose mandated primary mission is to ensure the security and resiliency of our nation's critical infrastructure, this thesis specifically examined the Department of Homeland Security as it followed the identical development process as the overall U.S. government in the post-9/11 era.

In the decade since 9/11, DHS was mandated to ensure the security of the nation's cyber-supported critical infrastructure that is predominantly privately owned. Chapter 4, Section A, presented evidence which suggests that DHS has consistently chosen to devote disproportionate budgetary resources to develop defensive technologies of questionable effectiveness, initiate redundant information sharing programs, and to develop cyber incidence response teams while not considering the utilization of component agency's legal authorities and capabilities, namely the U.S. Secret Service. To

provide recommendations to assist the department in developing a comprehensive cyber security methodology, an in depth analysis of the cyber-security mission and authorities of DHS was compared with the specific cyber authorities and capabilities of the USSS. The analysis indicated that the USSS has the expertise and legal mandate to integrate the traditional model of criminal investigation and deterrence to the realm of cyber security and support the DHS mission.[385]

Cyber-law enforcement effectiveness was also contrasted against the suitability and effectiveness of the militarization of cyberspace and the applicability of utilizing intelligence or military agencies to fulfill the nation's domestic cyber-security mission. Evidence presented indicates that DHS's apparent acceptance of the premise that NSA/DOD should provide technical assistance, cyber security support, mitigation, and cyber threat indicators, may be in violation of existing laws prohibiting the domestic operation of the intelligence community and military. Evidence identified within the literature review and elsewhere in this thesis also indicates that relying on the IC and military cyber attack forces to provide effective defensive indicators and information may be an false assumption because providing that information would be counter to the IC and military's primary mission and negatively affect their overall effectiveness. The analysis indicated that the government's proposed designation of all cyber attacks targeting the nation's critical infrastructure as a "national security" event was initiated and fully supported by the IC and military. This designation, regardless of the identity or motivations of the perpetrator, was described within this thesis as a thinly veiled attempt to provide justification for the entire IC to operate domestically despite the fact that the FBI is the only IC agency legally authorized to conduct domestic operations to counter national security threats. Finally, this proposal by the IC was presented as an effort that could threaten our citizens' privacy due to the lack of intelligence community operational oversight and the borderless nature of the cyber world.

Below, the thesis offers recommendations to support the formulation of government cyber-security policy that could develop the most effective, integrated cyber-

385 "DHS Cyber Component Overview," U.S. Department of Homeland Security, accessed January 19, 2014, www.dhs.gov.

security methods while continuing to effectively investigate and punish cyber attackers, deter future attacks, protect civil liberties, and the functionality of the Internet.

B. POLICY RECOMMENDATIONS

1. DOD/NSA must remain focused on nation-state cyber threats and foreign activities.

To ensure that the NSA, the nation's premier SIGINT collection agency, remains focused on the exploitation of foreign SIGINT and foreign espionage activities in support of our national security interests, as well as to protect our citizens' civil liberties, the agency must not be permitted to utilize its capabilities on domestic targets or systems. Additionally, the DOD cyber attack forces must not operate on or within domestic cyber systems, unless owned by the DOD, and must concentrate their activities to exploiting foreign vulnerabilities.

2. FBI must remain the only IC agency permitted to operate domestically with proper judicial oversight.

The Bureau's domestic cyber intelligence activity must be limited to the investigation of espionage threats which are committed by nation-state supported actors that 1.) Seek to gain knowledge from information systems which contain information of national security value or; 2.) Attack critical infrastructure systems to degrade or disrupt such systems to cause a national crisis. The FBI Cyber Criminal Division should continue to investigate cyber intrusions within their criminal jurisdictions.

3. DHS should continue to enhance its network defense capabilities and information sharing initiatives but must increase its utilization and reliance on the deterrent effect of USSS cyber criminal investigations as an integral part of the department's cyber security efforts.

Although, as indicated within this thesis, defensive technology can never be expected to thwart the most determined or advanced attackers, defensive technology does provide a high level of protection. As presented within the thesis, in recognition of the inherent vulnerabilities in cyber systems, deterrent law enforcement operations are necessary to ensure attackers are identified and apprehended.

C. FUTURE RESEARCH RECOMMENDATIONS

While this thesis provided a comprehensive review of a portion of the total cyber security issues confronting this nation and our current cyber security efforts, we must recognize that the cyber world is continuing to rapidly develop and expand its influence on our everyday lives. Additionally, as a nation, we must remain cognizant that the threats continue to expand as prospective attackers develop new tools, discover previously unidentified vulnerabilities in our critical systems, and find additional motivations to attack our nation's cyber-supported critical infrastructures.

In recognition of the unknown challenges waiting in our nation's future, additional research is required to support the development of adaptable policies scalable to the rapidly changing environment. A demonstrated through the literature review, the existing research into the threats against U.S. critical cyber infrastructure has generally focused on the two key areas of defensive security utilizing technology and offensive operations that identifies and eliminates the actors who seek to target our cyber systems.

P**o**ssible avenues of valuable research may also include a review of emerging technologies that provide more adaptable defensive precautions through leveraging artificial intelligence. At some point, it is possible that the technology will supplant the need for human decisions and intervention that is often identified as the point of failure during a post-intrusion review. Another area of valuable research may include a review of successful cyber security efforts initiated by the private sector, how the need for those efforts was advertised within the corporate structure to gather support, and the way that those successes could be imitated or initiated throughout the government enterprise. Related to this topic, a comprehensive study of the cyber security efforts of other nations and whether those efforts could be employed with the U.S. could prove beneficial to policy makers.

Finally, additional research regarding deterrence or game theory as it applies to low-level attackers; advanced/organized criminal actors, and nation-state supported cyber threats should be conducted to more thoroughly evaluate the effectiveness of offensive operations against attackers of different skill levels and motivations.

LIST OF REFERENCES

Anderson, Levon. "Countering State-Sponsored Cyber Attacks: Who Should Lead?" In *Information as Power: An Anthology of Selected United States Army War College Student Papers Volume 2*, edited by Jeffrey L. Groh, David, J. Smith, Cynthia E. Ayers, and William O. Waddell, 105–122. Carlisle Barracks, PA: U.S. Army War College, 2007.

Anderson, Ross. *Security Engineering: A Guide to Building Dependable Distributed Systems*. New York: Wiley, 2001. http://ieeexplore.ieee.org.libproxy.nps.edu/xpls/abs_all.jsp?arnumber=991552&tag=1.

Bazan, Elizabeth B. *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions* (CRS Report RL3046). Washington, DC: Congressional Research Service, February 15, 2007. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA447938.

Bjelopera, Jerome P., and Mark A. Randol. *The Federal Bureau of Investigation and Terrorism Investigations*. (CRS Report No. R41780). Washington, DC: Congressional Research Service, January 14, 2013. http://assets.opencrs.com/rpts/R41780_20110427.pdf.

Brenner, Susan W. "'At Light Speed': Attribution and Response to Cybercrime/Terrorism/Warfare." *Journal of Criminal Law and Criminology (1973-)* 97, no. 2 (January 1, 2007): 379–475. doi:10.2307/40042831.

———. "Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement?" *Bepress Legal Series*, August 6, 2003. http://law.bepress.com/expresso/eps/15/.

Bush, George W. "2002 State of the Union Address." *Business Source Complete*, Vital Speeches of the Day, 68, no. 9 (February 15, 2002): 5.

Byman, Daniel, and Benjamin Wittes. "Reforming the NSA." *Foreign Affairs*, April 17, 2014. http://www.foreignaffairs.com/articles/141215/daniel-byman-and-benjamin-wittes/reforming-the-nsa.

Cohen, Dara Kay, Mariano-Florentino Cuéllar, and Barry R. Weingast. "Crisis Bureaucracy: Homeland Security and the Political Design of Legal Mandates." *Stanford Law Review* 59, no. 3 (December 1, 2006): 88. doi:10.2307/40040307.

Curran, John. “DHS OIG Chides Cyber Office Over Planning Deficiencies.” *Cybersecurity Policy Report*, July 11, 2011. http://search.proquest.com.libproxy.nps.edu/docview/879014382/140CF1D28B6243B2AB/4?accountid=12702.

Defense Daily International. “FBI, Industry Fighting Back Against Cyber Attackers, Agency Official Says.” June 13, 2013.

Deffer, Frank. *Planning, Management, and Systems Issues Hinder DHS’ Efforts To Protect Cyberspace and the Nation’s Cyber Infrastructure*. (OIG -11-89). Washington, DC: OIG and DHS, June 2011. https://www.hsdl.org/?view&did=683172.

Doyle, Charles, and Jennifer Elsea. *The Posse Comitatus Act and Related Matters: A Sketch* (CRS Report R42659).Washington, DC: Congressional Research Service, August 21, 2012. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA462391.

Doyle, Charles. *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws (*CRS Report 97–1025). Washington, DC: Congressional Research Service, January 27, 2010.

Edwards, Charles. *Review of the Department of Homeland Security’s Capability to Share Cyber Threat Information* (OIG Report 11–117). Washington, DC: DHS-OIG, September 2011.

Emptywheel blog. “FBI: A Decade in Numbers.” September 14, 2011. http://www.emptywheel.net.

Enders, Walter, and Todd Sandler. “After 9/11: Is It All Different Now?” *Journal of Conflict Resolution* 49, no. 2 (April 1, 2005): 259–77. doi:10.1177/0022002704272864.

Finklea, Kristin M., and Catherine A. Theohary. *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement* (CRS Report R42547). Washington, DC: Congressional Research Service, July 20, 2012. United States. http://digital.library.unt.edu/ark:/67531/metadc98020/metadata/?q=cybersecurity%20cybercrime.

Fleming, Matthew, and Eric Goldstein. *An Analysis of the Primary Authorities Governing and Supporting the Efforts of the Department of Homeland Security to Secure the Cyberspace of the United States.* Arlington, VA: Homeland Security Studies and Analysis Institute, May 24, 2011. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2182675.

Flowers, Angelyn, Sherali Zeadally, and Acklyn Murray. “Cybersecurity and U.S. Legislative Efforts to Address Cybercrime.” *Journal of Homeland Security and Emergency Management* 10, no. 1 (April 13, 2013): 1–27.

Gartzke, Erik. “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth.” *International Security* 38, no. 2 (October 2013): 41–73. doi:10.1162/ISEC_a_00136.

Gonzales, Alberto. “Legal Authorities Supporting the Activities of the National Security Agency Described by the President.” January 19, 2006. http://web.elastic.org/~fche/mirrors/www.jya.com/2012/06/doj011906.pdf.

Goodman, Will. “Cyber Deterrence: Tougher in Theory Than in Practice?” *Strategic Studies Quarterly*, (2010): 102–35.

Hammond, Brian. “Cybersecurity Bill Would Clarify DHS Role, Create Info-Sharing Body.” *Cybersecurity Policy Report*, December 19, 2011.

Hare, F. “The Significance of Attribution to Cyberspace Coercion: A Political Perspective.” In *Proceedings of the 2012 4th International Conference on Cyber Conflict*, edited by Christian Czosseck, Rain Ottis, and Katharina Ziolkowski. New York: IEEE, 2012. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6243970.

Harlow, Richard. “Two Missions, One Secret Service: The Value of the Investigative Mission.” Master’s thesis, Naval Postgraduate School, 2011. www.hsdl.org/?view&did=691426.

Jaeger, Paul T., John Carlo Bertot, and Charles R. McClure. “The Impact of the USA Patriot Act on Collection and Analysis of Personal Information under the Foreign Intelligence Surveillance Act.” *Government Information Quarterly* 20, no. 3 (July 2003): 295–314. doi:10.1016/S0740-624X(03)00057-1.

Kaiman, Jonathan. “China Reacts Furiously to U.S. Cyber-Espionage Charges.” *Guardian*, May 20, 2014. http://www.theguardian.com/world/2014/may/20/china-reacts-furiously-us-cyber-espionage-charges.

Keely, David M. “Cyber Attack! Crime or Act of War?” Master’s thesis, U.S. Army War College, 2011. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA553344.

Lampson, Butler W. “Computer Security in the Real World.” *Computer* 37, no. 6 (June 2004): 37–46.

Lemieux, Frederic. *Investigating Cyber Security Threats: Exploring National Security and Law Enforcement Perspectives. Investigating Cyber Security Threats: Exploring National Security and Law Enforcement Perspectives.* Washington, DC: Cyber Security Policy and Research Institute, George Washington University, 2011. http://www.cspri.seas.gwu.edu/Seminar%20Abstracts%20and%20Papers/2011-2%20Investigating%20Cyber%20Security%20Threats%20Lemieux.pdf.

Lewis, James Andrew. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.* Washington, DC: Center for Strategic and International Studies, December 2002. http://www.steptoe.com/publications/231a.pdf.

———. *Securing Cyberspace for the 44th Presidency*. Washington, DC: Center for Strategic and International Studies, December 2008.

Libicki, Martin C. "Cyberspace Is Not a Warfighting Domain." *A Journal of Law and Policy for the Information Society* 8, no. 2 (2012): 325–439.

———. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND, 2009. http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=304894.

Lynn, William F, III. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs*, September/October 2010. http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

Martin, Nigel, and John Rice. "Cybercrime: Understanding and Addressing the Concerns of Stakeholders." *Computers & Security* 30, no. 8 (November 2011): 803–814. doi:10.1016/j.cose.2011.07.003.

McHugh, John, Alan Christie, and Julia Allen. "Defending Yourself: The Role of Intrusion Detection Systems." *IEEE Software.* September/October 2000, 42–51.

Moore, Tyler, Allan Friedman, and Ariel D. Procaccia. "Would a 'Cyber Warrior' Protect U.S.: Exploring Trade-Offs between Attack and Defense of Information Systems." In *Proceedings of the 2010 Workshop on New Security Paradigms 10* New York: 2010 ACM, 2010. doi:978-1-4503-0415-3.

Moteff, John. *Critical Infrastructures: Background, Policy, and Implementation. Congressional Research Office (*CRS Report RL30153). Washington, DC: Congressional Research Service, February 21, 2014.

Mueller, Robert. "Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies." Federal Bureau of Investigation, March 1, 2012. http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

Myers, Elizabeth A. *Cyber as a' Team Sport': Operationalizing a Whole-Of-Government Approach to Cyberspace Operations*. Master's thesis, National Defense University, 2011. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA545638.

Nakashima, Ellen, and William Wan. "U.S. Announces First Charges against Foreign Country in Connection with Cyberspying." *Washington Post*, May 19, 2014. http://www.washingtonpost.com/world/national-security/us-to-announce-first-criminal-charges-against-foreign-country-for-cyberspying/2014/05/19/586c9992-df45-11e3-810f-764fe508b82d_story.html.

Nakashima, Ellen. "Obama Signs Secret Directive to Help Thwart Cyberattacks." *Washington Post*, November 14, 2012. http://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html.

National Commission on Terrorist Attacks upon the United States. "9/11 Commission Report—Executive Summary." National Commission on Terrorist Attacks upon the United States. National Commission on Terrorist Attacks upon the United States. Accessed September 25, 2014. http://govinfo.library.unt.edu/911/report/911Report_Exec.htm.

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report*. Washington, DC: Government Printing Office, July, 22, 2004. http://govinfo.library.unt.edu/911/report/index.htm.

National Security Council. *Cyberspace Policy Review: Securing America's Digital Future*. New York: Cosmo Reports, May 2009.

Nolan, Andrew, and Richard M. Thompson, III. *Reform of the Foreign Intelligence Surveillance Courts: Procedural and Operational Changes* (CRS Report No. R43362). Washington, DC: Congressional Research Service, January, 16 2014. http://digitalcommons.ilr.cornell.edu/key_workplace/1228/.

O'Connell, M. E. "Cyber Security without Cyber War." *Journal of Conflict and Security Law* 17, no. 2 (August 8, 2012): 187–209. doi:10.1093/jcsl/krs017.

Pal, Ranjan, and Leana Golubchik. "Analyzing Self-Defense Investments in Internet Security under Cyber-Insurance Coverage." In *2010 IEEE 30th International Conference on Distributes Computing Systems*. doi:10.1109/ICDCS.2010.79.

Pasquali, Valentina. "Growing Threat." *Global Finance* 27, no. 5 (May 2013): 20–24.

President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures.* Washington, DC*:* President's Commission on Critical Infrastructure Protection, October 1997.

PwC. *2014 U.S. State of CyberCrime Survey. Annual State of Cybercrime Survey*. London: PricewaterhouseCoopers, June 2014. http://www.pwc.com/us/en/increasing-it-effectiveness/publications/2014-us-state-of-cybercrime.jhtml.

———. "Cybercrime Incidents, Associated Financial Costs Surge While Organizations Still Unprepared to Battle Threats, According to 2014 U.S. State of Cybercrime Survey from PwC and CSO." May 28, 2014. http://www.pwc.com/us/en/press-releases/2014/cybercrime-incidents-associated-financial-costs-surge.jhtml

Randazzo, Marisa R., Michelle Keeney, Eileen Kowalski, Dawn Cappelli, and Andrew Moore. *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*. Pittsburgh, PA: Carnegie Melon Software Engineering Institute, 2005. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA441249.

Reese, Shawn. *The U.S. Secret Service: An Examination and Analysis of Its Evolving Mission*. Washington, DC: Congressional Research Service, July 31, 2008.

Rice, Mason, Robert Miller, and Sujeet Shenoi. "May the U.S. Government Monitor Private Critical Infrastructure Assets to Combat Foreign Cyberspace Threats?" *International Journal of Critical Infrastructure Protection* 4, no. 1 (April 2011): 3–13. doi:10.1016/j.ijcip.2011.02.001.

Rid, Thomas. "The Great Cyberscare: Why the Pentagon Is Razzmatazzing You about Those Big Bad Chinese Hackers," *Foreign Policy*, March 13, 2013.

Rivera, Matthew. "Deterrence in Cyberspace." Master's thesis, Joint Forces Staff College, June 13, 2012. www.dtic.mil/dtic/tr/fulltext/u2/a562428.pdf.

Rollins, John, and Anna Henning. *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations* (CRS Report No. R40427). Washington, DC: Congressional Research Service, March 10, 2009.

Saydjari, O. Sami. "Cyber Defense: Art to Science." *Communications of the ACM* 47, no. 3 (March 2004): 52–57.

———. "Defending CyberSpace." *Computer* 35, no. 12 (December 2002): 125–27.

Shachtman, Noah. "Military's Cyber Commander Swears: 'No Role' in Civilian Networks. *Wired*, September 23, 2010.

Sofaer, Abraham D., and Seymour E. Goodman. “Cyber Crime and Security. The Transnational Dimension.” In *The Transnational Dimension of Cyber Crime and Terrorism*, edited by Abraham D. Sofaer and Seymour E. Goodman, 1–34. Stanford, CA: Hoover Institution Press, 2001. http://media.hoover.org/documents/0817999825_1.pdf.

Sommestad, Teodor, Mathias Ekstedt, and Pontus Johnson. “Cyber Security Risks Assessment with Bayesian Defense Graphs and Architectural Models.” In *42nd International Conference On System Sciences, 2009*, edited by Ralph H. Sprague Jr., Piscataway, NJ: IEEE, 2009. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4755419.

Tomisek, Steven J. *Homeland Security: The New Role for Defense.* Washington, DC: Institute for National Strategic Studies, National Defense University, 2002.

Trustwave. “2013 Trustwave Global Security Report.” *Trustwave*. Accessed October 2, 2013. https://www2.trustwave.com/2013GSR.html.

U.S. Department of Homeland Security (DHS). “2011 DHS Budget in Brief.” February 2011. http://www.dhs.gov/xlibrary/assets/budget_bib_fy2011.pdf.

———. “2013 DHS Budget in Brief.” February 2013.

——— *Bottom-Up Review.* Washington, DC: DHS, July 2010. http://www.dhs.gov/bottom-review.

——— “Preventing and Defending Against Cyber Attacks.” September 2010. http://www.dhs.gov/xlibrary/assets/preventing-and-defending-against-cyber-attacks.pdf.

——— *Quadrennial Homeland Security Review (QHSR).* Accessed September 26, 2014. http://www.dhs.gov/quadrennial-homeland-security-review-qhsr.

———. “2009 DHS Budget in Brief.,” February 4, 2009.

———. *Blueprint for a Secure Cyber Future*. Washington, DC: DHS, November 2011. http://www.dhs.gov/blueprint-secure-cyber-future.

———. “Secretary Michael Chertoff U.S. Department of Homeland Security Second Stage Review Remarks,” July 13, 2005. http://www.dhs.gov/xnews/speeches/speech_0255.shtm.

———. *Quadrennial Homeland Security Review*. Washington, DC: Department of Homeland Security, February 2010. https://www.hsdl.org/?view&did=29742.

———. *National Infrastructure Protection Plan*, Washington, DC: DHS, 2009. https://www.dhs.gov/national-infrastructure-protection-plan.

———. *One Team, One Mission, Securing Our Homeland: U.S. Department of Homeland Security Strategic Plan, Fiscal Years 2008–2013*. Washington, DC: DHS, 2008. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA487194.

U.S. Department of Homeland Security (DHS) and Office of Inspector General (OIG). *U.S. Computer Emergency Readiness Team Makes Progress in Securing Cyberspace, but Challenges Remain*. Washington, DC: DHS and OIG, June 2010.

U.S. Department of Justice, "Attorney General's Guidelines for Domestic FBI Operations." September 29, 2008. http://www.justice.gov/sites/default/files/ag/legacy/2008/10/03/guidelines.pdf.

U.S. Federal Bureau of Investigation. "Ten Years after 9/11–Cyber." May 19, 2014. http://www.fbi.gov/about-us/ten-years-after-the-fbi-since-9-11/just-the-facts-1.

———. *The FBI: A Centennial History, 1908–2008*. 2nd ed. Washington, DC: U.S. Government Printing Office, 2008. http://www.fbi.gov/about-us/history/a-centennial-history.

U.S. Government Accountability Office (GAO). Critical *Infrastructure Protection Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities: Report to Congressional Requesters* (GAO-05-434) Washington, DC: GAO, May 2005.

———. *Critical Infrastructure Protection: DHS Needs to Better Address Its Cybersecurity Responsibilities* (GAO-08-1157T). Washington, DC: GAO, Sept. 16, 2008. http://www.gao.gov/products/GAO-08-1157T.

———. *DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise* (GAO-08-825 Washington, DC: GAO, September 2008. https://www.hsdl.org/?view&did=235401.

U.S. Secret Service. "United States Secret Service Signs Partnership Agreement with Italian Officials Establishing the First European Electronic Crimes Task Force." July 6, 2009, http://www.secretservice.gov/press/GPA05-09_EuropeanECTF.pdf.

Verizon Enterprise Solutions. "2013 Data Breach Investigations Report." Accessed September 29, 2013. http://www.verizonenterprise.com/DBIR/2013/.

Weimann, Gabriel. *Cyberterrorism: How Real Is the Threat*? Washington, DC: United States Institute of Peace, 2009. http://dspace.cigilibrary.org/jspui/handle/123456789/15033.

White House, The. “Presidential Policy Directive 21: Critical Infrastructure Security and Resilience February 12, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

———. “Presidential Policy Directive 8: National Preparedness.” March 30, 2011. https://www.hsdl.org/?view&did=7423.

———. “The Comprehensive National Cybersecurity Initiative.” Accessed September 26, 2014. http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

———. *National Strategy to Secure Cyberspace*. Washington, DC: White House Office, February 2003. https://www.hsdl.org/?view&did=1040.

Wilshusen, Gregory C., and Nabajyoti Barkakati. *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented* (GAO-13-187). Washington, DC: Government Accountability Office, February 14, 2013. http://www.gao.gov/products/GAO-13-187.

Wilson, Clay. *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*. Washington, DC: Congressional Research Service, January 29, 2008.

Young, Mark D. “National Cyber Doctrine: The Missing Link in the Application of American Cyber Power.” *Journal of National Security Law & Policy* 4, no. 173 (2010): 173–96.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California